NIST Government Contractor Report
NIST/GCR -93-635
September 7, 1993

PRIVATE BRANCH EXCHANGE (PBX) SECURITY GUIDELINE

National Institute of Standards and Technology
Computer Systems Laboratory
Open Telecommunications Security Project
Integrated OSI, ISDN, and Security Program

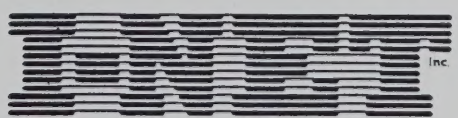


TABLE OF CONTENTS

1.0 Introduction

Telecommunication digital switch technology has advanced rapidly in the last few years. While the topic of mainframe and table top computer security has received much attention the last 20 years, the security capability of telecommunications hardware and software, specially the Private Branch Exchange (PBX) has not kept pace.

The challenge in PBX security lies in securing the data and features of the PBX and related equipment. Not only is the PBX able to process internal calls and provide access to the public switched network, but advance features such as Direct Inward System Access (DISA) allow subscribers to remotely obtain PBX dial tone and re-originate telephone calls. Hackers have taken advantage of the DISA feature to fraudulently obtain millions of dollars worth of long distance usage which is billed to unsuspecting PBX owners.

For the purpose of this document, role definitions are provided as follows:

User - one who has the ability to access, modify, add, or delete PBX switch data. Access may be via directly connected terminals and/or dial up ports. Users may be authorized (e.g. employees) or unauthorized (e.g. hackers).

Subscriber - one who has access to telecommunications devices such as phones, FAX, Voice Mail, Automatic Call Distributor (ACD) via voice switching. Those who have access to non-telecommunications related computers are also considered subscribers.

Operations, Administration, and Maintenance Personnel (OA&M) - those who have access to the PBX switch and/or data to perform testing, repair, define/modify/delete subscriber functions and call processing.

Hacker - one who does not have any authorization to act as a user or subscriber to the PBX.

Intruder - one who has legitimate access to be either a user and/or a subscriber of the PBX but does (or attempts) any unauthorized activity (e.g. attempts to change a class of service).

1.1 Purpose

The purpose of this document is to describe the basic concepts of PBX security. Telephone switching technology has grown dramatically since its early days. During the era of analog switching, security measures were not necessary since only hard wired changes could change switch operations. Its main purpose was to provide the means of distributing voice communication and features were limited to either direct-dial or

operator-assisted calls. In today's highly advanced and rapidly evolving 'digital switch' technology, switch integrity has become more of an issue. Switch equipment owners are more aware of problems that arise from inadequate security measures because of loss of revenues, assets, or loss of control of their assets. The losses occur when the switching system is penetrated (intentionally or unintentionally) and the penetration causes scenarios such as: loss or disruption of service (availability), unauthorized manipulation of switch database (loss of integrity), malicious use of features, industrial espionage (loss of confidentiality), or toll fraud. Since telephone switching systems require a relatively large capital investment, owners are aware that these assets need to be protected and that the security measures must be cost effective.

1.2 Topics of Discussion

To broaden and emphasize switch security, it is important to be aware of certain facts about and limitations of the PBX network. The following subjects will be covered in this document. Section 2 is a general, high-level description of a telephone switch system. This will include topics in the use of the switch, switch technology, transmission technology, and types of signalling between equipment. Section 2 also discusses the various hardware and software assets involved in telephone switch systems. Section 3 covers additional assets that are external to the PBX switch. Section 4 will cover the various threats the switch must be protected against. Section 5 will discuss how vulnerable and/or susceptible the switch is to specific threats. Section 6 will point out that telephone switching systems have their own built in hardware/software protection packages. Section 7 will discuss the functions of the PBX administrator (or PBX security administrator). Section 8 is a list of figures used to highlight the narratives. Section 9 list all the resources used for this document. Section 10 lists the abbreviations and glossary of common telecommunications and security terms. Appendix A shows an example of a security policy and some controls needed to secure the PBX environment. And Appendix B list a security assessment checklist.

2.0 Switch System Technology

Telephone private branch exchanges (PBX) are in many ways similar to computer systems and PBX technology has followed the same development path. It starts out with structured software and hardware architecture. Advancements in technology can then be implemented using modular techniques of enhancements. Advanced features providing added value to the subscriber could be easily implemented through software enhancements and modular hardware upgrades.

2.1 PBX System Purpose

With the advancement of telephone switch technology, equipment and features that were once the sole domain of the telephone central office can now be established for use by private entities. The concept of having all telephone instruments (stations) physically connected to local central offices is a thing of the past. Groups of customers (eg. hospitals, hotels, and companies) can now provide telephone service to their employees at an economical rate using a PBX system. These organizations will buy/lease the switching equipment with a preset number of customer lines, features, and outside access (trunks). They are then able to administer their telephone services and tailor it to their own needs through software or hardware modifications. See Figure 1 (Typical PBX Network Connections), Figure 9 (PBX as part of the PSN), and Figure 10 (PBX as Part of a CCS7 Network).

EXAMPLE:

> Organization XYZ has 100 members. They are the sole tenants of Building ABC. After a thorough study of organizational and member needs, they have decided it is not economical for them to provide each member a hard-wired connection to the local central office. Instead, they will buy/lease a PBX with the following switch parameters. They will have 20 dedicated outside trunks connected to the local central office [7 incoming call trunks, 7 local only outgoing call trunks, 4 2-way trunks which carry both incoming and outgoing calls, and 2 direct long distance calling trunks (MCI, Sprint, AT&T, etc.)]. The PBX will provide each member with their own extension number for direct inward dial (DID) calls. All long distance calls will go through the attendant console operator. Local outside calls can be accessed by dialling '9' and the number to be called. They will be provided such features as extension calling, 'call-waiting', 'last number redial', 'intercom', etc.. Future upgrades would require purchase of additional modular hardware and software (such as Integrated Services Digital Network (ISDN) features) needed to support the new requirements.

Because organizations now have more control of their telephone assets, they can grow and provide more features and capabilities as the need arises. PBXs are the means by

which organizations can utilize the telephone technology, be flexible enough to tailor for their own needs, are not controlled in the local central office, and are still economical.

2.2 Basic Telephone System Technology

Equipment associated with any generic telephone switch can be broken down as follows:

1. signalling
2. control
3. switching matrix.

The signalling equipment monitors the activities of the incoming and outgoing lines and trunks and passes along the appropriate status or control information to the control element of the switch. The control equipment then processes these incoming and outgoing signals and sets up, modifies, or takes down the appropriate call connections. The Switching equipment provides a switching matrix. This is a network of selectable real or virtual paths used to connect the calls between the input and output circuits (i.e. lines and/or trunks).

2.2.1 Subscriber Line Assignment

Every DID subscriber line location in the PBX switch is assigned a unique 10-digit number. Telephone connections are based on the North American Numbering Plan (NANP). It is designated as NPA-NXX-YYYY. NPA represents a geographical location (area code). NXX represents the office code of a particular exchange which process the calls for the station number YYYY. The last 4 digits, YYYY, is the station number and is associated with a circuit physically connected from the subscriber station to the PBX. See Figure 2 (North American Numbering Plan).

Certain group of numbers (YYYY) can be assigned to certain functionalities. '0000 -0099' can be assigned as switch maintenance numbers. '0100 - 0999' can be assigned to 'Engineering'. '1000 - 1999' can be assigned to 'Human Resources'. The different groupings are based upon the organization's requirements.

Every PBX switch contains many circuit types. The major circuit types are lines, trunks, and service circuits. Lines are the physical connection between the PBX and the subscribers. 'Ringing current' capability is always present on these line circuits. Subscriber's on/off hook conditions are monitored. Trunks are physical connections from the PBX to other private, public, or interexchange carrier networks. It enables any telephone to be connected to any other telephone. Service circuits are circuits other than lines or trunks. There are different kinds of service circuits. The most common ones are: recorded announcement, loop around circuits, open and short circuit test circuits.

2.2.2 Digital System

Digital telephone switching system assets are of modular design in both hardware and software. The main PBX modules are: CPU (Control), Memory, Network (Switching), Peripheral Equipment , and Input/Output Control . The main software functions are: Operating System, Maintenance, Switching Translations, and Administration. See Figure 3 (Modular Switch Components). This type of design allows flexible growth in processing capability, system interface, and increased switching capacity. It uses stored programs and time division multiplexing to convert analog voice signals (from the telephone handset) to digital representation and then back again. Digital technology makes possible the simultaneous transmission of voice and data at high speeds. The main hardware and software assets are listed as follows.

PBX Modules:

1. CPU (Control) Module - This module is the 'heart' of the PBX. It contains the software and hardware necessary to control the PBX. There is normally a redundant system of CPUs. One CPU is in the active processing mode and the other is in the 'hot' processing standby mode. They are synchronized to the same clocking source and are processing all calls at the same time. In case of failure in the active CPU, the standby CPU will become active while simultaneously placing the failed CPU in the standby mode. There may not be a subscriber awareness of a change in CPU activity.

2. Memory Module - This module stores all the information available in the switch. This includes read only memory (ROM), programmable read only memory (PROM), and random access memory (RAM). The system operating software resides here. Other examples of types of information stored in the memory module are telephone number assignments, call routing, trunk configuration, and system specifications.

3. Network (Switching) Module - This module is where the actual 'switching' of calls takes place. It contains its own memory to handle the call connection.

4. Peripheral Equipment Module - This module physically connects the outside trunks and telephone instruments to the PBX. It can also house special circuits, miscellaneous circuits such as voice announcements, conference calls, and test circuits. It also performs the basic inter-module signalling.

5. Input/Output Control Module - This module controls all connection from external devices, such as call detail recorders, maintenance and

administration terminals, modems, disk storage devices, and magnetic tape storage devices.

Software Functions:

1. Operating Systems - This is the main operating software of the PBX and provides high level command processing. This is the fixed 'base' program created by the vendor. Data in this system is modified via patches or parameter changes.

2. Maintenance - This system provides a more detailed syntax for the overall maintenance of the PBX hardware and software. Alarms and logs are part of this system

3. Switching Translation - This is the specific software/firmware that tells the PBX how to route all call connections. Subscriber and trunk data are part of this system.

4. Administration - This system performs such tasks as database manipulation control, storage device administration, and printing of database hardcopies. Permitted users and their privileges, printers and storage device type and device function are part of this system.

2.3 Advantages of Digital Switching

1. Since voice is encoded digitally, the voice portion of the call is less susceptible to noise and loss. Via Net Loss (VNL) in the digital network is 0 dB.

2. The CCS7 network can determine line and equipment state prior to completing call set up, using less facilities and allowing slow and fast busy tone to be sent in the originating office without holding up equipment in other offices.

3. Additional services can be provided such as last number redial, call waiting, call forwarding, 3-way calling, or repeat calling (i.e. notifying a calling subscriber when a called line becomes idle).

4. Security through the use of features such as selective call acceptance that denies calling access to lines with calling numbers that are not defined on the permitted caller list.

5. Multiple channel calling using Frame Relay and Wideband switching is possible. These features allow the rapid transfer of data (e.g. computer files and video images).

6. Performance monitoring - Using such things as framing information, the switch can monitor calls, facility activities, and report unacceptable results.

2.4 Disadvantages of Digital Switching

1. The switching equipment is more sensitive to building environment (i.e. dust, heat, cold, or humidity).

2. It is harder to diagnose/correct faults. It also requires a higher skill level, knowledge of architecture, and may require some sophisticated tools for testing.

3. Inadvertent activities are harder to detect. Issuing wrong commands, deleting/modifying wrong data may significantly reduce call processing without creating an alarm condition.

4. Malicious activities may be harder to detect if the security controls are not properly implemented.

2.5 Transmission Technology

There are two types of communications transmission involved in telephony: analog and digital. Analog signals are continuous, variable waveforms. Digital signals are discrete steps and of definite size or number. Analog transmission systems use tones to represent their data while digital transmission systems use digital pulses to represent data.

Analog signals must be periodically amplified to prevent degrading if it is transmitted over long distances. The problem is that the whole signal, even noise, gets amplified which distorts the signal even more. Digital signals, on the other hand, are unaffected by noise. Digital signals do not need re-amplification but are actually regenerated, which eliminates noise.

2.6 Signalling Process

Telephone usage is basically subscriber controlled. The subscribers, depending upon the type of call made, will 'send' the signal to a vast network of transmission and switching facilities. Various signals are sent to control PBX operation and also to indicate subscriber status to the network. The three general functions of signalling in modern telephony are:

1. Alerting - deals primarily with request for service, facility, or action of some kind. The action of picking up the telephone handset alerts the PBX that a calling subscriber will make a phone call. The PBX alerts the called subscriber of an incoming call by sending ringing voltage to the telephone station.

2. Transmitting the subscriber's address information - when a subscriber picks up his handset and receives dial tone, his address (specific line equipment number) is determined by the PBX. This gives the PBX access to the subscriber's list of features or options. The subscriber dials the number he wants to connect to. This is the information the PBX needs to route the call. Breaking (removing) dial tone indicates the PBX is receiving the dialed information.

3. Supervision - the PBX needs to know when lines or trunks are being accessed, or in use (busy), or not in use (idle). If in use, the PBX also needs to know when to release them for other calls. Line and trunk states are supervised.

2.6.1 Subscriber Loop

The subscriber picks up the handset (goes off-hook) which completes a loop to the PBX. Going off-hook is interpreted by the PBX as a request for service. This alerts the PBX which then sends dial tone to the caller. The PBX waits for the proper signal (dialing) from the telephone. Once dialing is completed, if the call is local, the PBX will check the called number to see if it is busy. If it is, it sends a busy signal to the calling party. If the called number is not busy, the PBX will establish the proper connections. It will signal the called party by sending ringing current to the called party's telephone. When the called party goes off-hook, that is the signal for the PBX to discontinue ringing and establish a talk path between the called and calling party. While conversation is going on, the PBX monitors the connection. When either party hangs up (goes on-hook), the PBX will release the connection and start monitoring again for alerting signals.

2.6.2 In-Channel Signalling

In-channel is also sometimes referred to as 'per trunk' signalling. It uses the same transmission facilities or channels for signalling and for voice. It can be further divided into two types: in-band and out-of-band signalling. In-band signalling transmits the signals in the same band of frequencies as the voice bands. This type of signal can be transmitted on any voice transmission media but has the problem of mutual interference between the signalling waveform and the voice itself. The most common example of in-band signalling is the 2600 hertz tone on-hook indication. Another example of this is the Dual Tone Multi Frequency signals sent out by the telephone during dialing. Out-of-band signalling uses the same facilities as the voice channel but not the same frequency band. One example of this type of signalling is when the telephone uses a rotary dial. This method sends out pulses with the number of pulses coinciding with the number dialed.

2.6.3 Common Channel Signalling

Common channel signalling is the process by which all the signalling is routed to a separate channel (path) that is different from the actual voice (conversation) channel. This provides for faster and 'cleaner' signalling. This type of signalling can be used when

there is a need to connect two separate PBX exchanges. Common channel signalling allows PBXs to communicate with each other and exchange information such as line/trunk availability and addresses. With common channel signalling, data signals are sent back over the data path, and the messages (such as busy tone, recordings) are generated at the 'local' PBX, thereby freeing voice channels for actual conversations. See Figure 4 (Common Channel Signalling)

The advantages of common channel signalling are:

1. only one set of signalling facilities are required for each trunk group;

2. single dedicated control channel allows for transfer of signalling information between control elements;

3. less prone to fraudulent acts since the control channel of common channel systems are not as accessible to subscribers and non-system users;

4. connections can be set up more rapidly between switching systems; and

5. the path used for common channel signalling does not have to be associated with/dedicated to a particular trunk group.

The disadvantages of common channel signalling are:

1. if one node fails to relay the disconnect information properly, facilities downstream from the disconnect will not release;

2. there is no automatic test of the voice circuit during call setup, each circuit has to be tested individually and done [1/n] times; and

3. all 'call information' is concentrated in one area (e.g. Signal Transfer Points).

3.0 Additional Switch Assets

Before beginning any type of security evaluation, it is important to first recognize what assets are considered part of the PBX network system. Second, it is important to distinguish the placement and/or priority of the value of these assets. Development of priorities will take into consideration the effects of hardware/software changes (whether it was intentional/unintentional and malicious or not) to the PBX network. There are two basic division of assets: hardware and software. The major PBX exchange modules and software functions are described in Section 2.2.2. Additional assets that could be considered as part of the PBX network are: attendant consoles, telephone stations, transmission media between the peripheral module and the subscribers, office records (e.g. PBX configuration, number assignments, location of subscribers, subscriber features, cable cross-connect assignments, etc.), telephone directory, modems, maintenance and administration terminals, and external distributed processing devices for call detail recording.

3.1 External Hardware Assets

These assets will comprise equipment that is external to the main PBX switch. See Figure 1 (Typical PBX Switch Network Connections).

1. Operation , Administration, and Maintenance (OA&M) Terminals - These terminals are connected to the PBX. They are used by the PBX administrator, switch technicians and engineers, and service order personnel. These terminals are used for maintaining the switch, checking alarm conditions, database and configuration changes, applying software patches to the operating system, and viewing of the overall integrity of the PBX. Since this equipment is connected to the PBX, the PBX is highly vulnerable to malicious action at OA&M terminals. These terminals should be protected and secured from any external or internal threat.

2. Distributed Peripheral Processors -These processors typically collect call detail recordings and other call information, logs, operational measurements, and other subscriber and user activities for use by the PBX administrator and other authorized users. These processors should also be secured so that only authorized personnel are allowed to view and manipulate the data.

3. Digital Cross-connect System (DSX) - Any high speed, digital signalling between the PBX and other adjunct equipment (trunks to the Central Office (PSTN)) that requires a 'clean' transmission media and a point of demarcation for testing is typically connected to this equipment. From this position, a person can monitor, test, and re-route any circuit or call-connections which is passing through it. The equipment should be in a secure area with only authorized personnel allowed access to it.

4. Main Distribution Frame (MDF) - All analog voice grade connections between the PBX and the telephone stations or analog trunks to the PSTN will be terminated at this equipment. This is a point of demarcation between the outside (PSTN) world and the PBX. From this position, a person can monitor and test any circuit or call-connection which is passing through it. The MDF should be in a secure area with only authorized personnel allowed access to it.

5. Intermediate Distribution Frame (IDF) - All typical voice grade connections between trunks to the PSTN may be terminated at this equipment. The IDF is typically used for in-house analog trunking of circuits. It is also a point of demarcation between the outside (PSTN) world and the PBX. From this position, a person can monitor and test any circuit or call-connection which is passing through it. The IDF should be in a secure area with only authorized personnel allowed access to it.

6. Attendant Consoles - This position is where you would find the typical PBX 'operator'. The function of an attendant is to process incoming and outgoing calls that subscribers are not permitted to handle directly. Operators normally have full access to all trunks. Training should be given to these operators that will ensure proper: processing of calls; use of trunks; and services allowed to subscribers. From the attendant console position, a person can monitor calls. The attendant console need not be in a secure area because it basically performs the same functions as a 'super' telephone station. Any telephone station can have a set or subset of features which an attendant console has. Care should be exercised so that passwords or codes for controlled functions are not compromised.

7. Telephone Stations - This is the instrument by which subscribers can make/receive calls. A number is assigned to a specific station (single or multiline station). A set of features and privileges are also assigned to this number. Examples of features and privileges the PBX can offer include access to toll-free trunks, speed dial calling, and conference calls. Care should be exercised so that passwords or codes to certain features and privileges are not compromised.

3.2 Office Documentation

These assets comprise the necessary documentation needed for the proper operation, administration, and maintenance of the PBX and the network. Disclosure or unauthorized use of these documents can result in unauthorized access which can result in substantial damage to the PBX and the switch network, degradation of service, or even loss of service. Only authorized personnel should be allowed access to this documentation.These hardcopies consist of:

- original equipment manufacturer's (OEM) manuals, software code, and documents.

- telco generated paper records of telephone directories, line and trunk configuration and equipment location, list of authorized users (remote and on-site), switch configuration, network configuration, service order requests, trouble logs, audit logs, exception reports, and maintenance logs.

4.0 Threats

Understanding the motivation, capabilities and techniques for unauthorized access/use of a PBX will be useful when attempting to mitigate/remove threats. Good security techniques are necessary because the threats posed have changed in recent times. Hackers were originally only attempting to gain access and 'map' information on the switches they successfully penetrated. Criminals have now found communications: that are difficult to trace, that do not have to be paid for, and which appear to be part of the trusted network. They are willing to pay for network access information. Hackers are now gaining monetary rewards for providing network access as opposed to peer 'recognition' that was the former motivating force driving them. The use of abundantly available technology has also made attacks much easier. Examples of these technologies are: video recorders used in public places to capture DISA access codes; high power, low cost computers and modems; Programmable Read Only Memory (PROM) burners; and CCS7 analyzer equipment. See Figure 6 (Basic Threat Evaluation Process) and Figure 7 (Modification of the FIPS 102: Certification Process).

The PBX is threatened in several areas:

1. The voice mail system is attacked and either held hostage for ransom or used for illegitimate purposes (e.g. arranging drug deals).

2. Unauthorized DISA use which has resulted in huge phone bills to the PBX owners.

3. Unauthorized modification of data which requires time and effort by the PBX owner to verify the data and correct/update/remove unauthorized data/changes.

4. Unauthorized physical access to material and data that results in stolen equipment and information that can be used to perpetrate further unauthorized access to the PBX through voice mail, DISA, and OA&M ports.

Threats will be considered any circumstance, condition, or event with the potential to cause harm to the PBX switch system resources in the form of destruction, disclosure, modification of data, denial of service, abuse, and/or fraud.

This definition includes the concept of a threat objective (the intended impact or the result desired from executing a threat). Threat objectives will include unauthorized use (theft) of telephone services and capabilities, unauthorized intercept of information/data being transmitted, corruption of information/data being transmitted, and/or disruption or destruction of telephone services and capabilities. These threat objectives will be addressed in terms of their impact on **confidentiality, integrity and availability** of a PBX.

Confidentiality relates to the concept of holding the PBX voice/data transmissions in confidence. Threats to confidentiality may be thought of as falling into two basic groups: inadvertent disclosure and deliberate circumvention. Inadvertent disclosure is usually associated with accidental misrouting of transmissions, but can occur as the result of a malicious act. Deliberate circumvention is done by unauthorized monitoring.

Integrity is the concept of being able to assure that information/data or voice transmissions can be maintained in an unimpaired condition and is not subjected to unauthorized modification whether that modification is intentional or inadvertent. Threats to integrity affect the ability of the PBX switch to provide the users and/or subscribers with the quality of services and functionality that they are expecting. In addition, threats to integrity affect the ability to ensure that the transmission is routed to the destination for which it is intended. Integrity threats also include subversion. Subversion involves the introduction of unauthorized changes to the operating system or the software processing in any one of the PBX components. Examples of subversion include the introduction of Trojan Horses or Viruses. Subversion is potentially the most serious of the threats to integrity, since it can lead to massive information/data loss or the continuous unauthorized exploitation of switch capabilities.

Availability is the concept of assuring that the hardware and software assets of the switch are available to the subscriber at the time the subscriber needs them, and in the form that they are needed. This can usually be accomplished by taking actions necessary to assure operation in the face of single point failures without incurring costs beyond reasonable levels.

4.1 Threat Selection and Organization

Generic threats to the PBX switch system were derived from a large basic list of generic threats generally recognized within the security community as applicable to both computer systems and telecommunications systems. Major parameters considered include:

1. The maintenance of an open environment required by a telephone system providing a full range of capabilities to subscribers,

2. the data transmission capability of a voice switch,

3. the digital nature of the PBX, focusing on development, testing and installation of software controlling the PBX functionality at all levels,

4. the operation and maintenance of the PBX, and

5. the interface of the PBX with remote devices (e.g., other voice switches,

computer systems, remote terminal devices, etc.).

This approach was used since the PBX switch system represents an integration of many functionalities that are associated with both computer and telecommunications systems.

The threats selected are listed in Figure 5. These threats are organized as categories of human and physical threat sources. Further, Figure 5 reflects the relationship of each threat to the threat objectives of confidentiality, integrity, and availability.

4.2 Human Threat Sources

Human threats include: malicious attacks, theft of PBX equipment (hardware and software), sabotage, security feature bypass, unauthorized access to the PBX, unauthorized manipulation of database, misrouting of calls, disruption of service, unauthorized disclosure of switch data and technology, failure to identify and diagnose errors and failures, negligence, and switch failure due to improper maintenance.

4.2.1 Employee or Insider

Intentional or accidental employee errors, omissions, or malicious acts can account for 50% of the damages or losses experienced by an organization. Insider threats come from employees or personnel with authorized access to the PBX network hardware and software. Whether by accident or omissions, human error by 'insiders' is by far the most costly and where the greatest loss is incurred. Security awareness can be emphasized by requiring employee accountability and by limiting user access only to assets required in the normal performance of duties. This is the most significant of all threats because many users have authorized access to the PBX network. Security checks and background investigations (e.g. NAC & I) should be conducted for personnel working in sensitive areas. Security awareness training should be provided for all employees. Use built in PBX security features, if possible, to check and verify employee input and thereby reduce mistakes which could adversely impact PBX system performance.

4.2.2 Hackers or Outsider

Outsider threats come from persons with unauthorized access to the PBX network hardware equipment and software. Their access will always be considered illegal, malicious, and may be detrimental to the proper operation of the PBX network. These external threats can be carried out by 'hackers'. Hackers are individuals who attempt to gain unauthorized access to the PBX network. Their primary purpose for access is for personal satisfaction, industrial espionage, malicious destruction of property, for profit, or malicious use of property. The PBX system is increasingly migrating to the "open system" software/hardware architecture. This architecture increases the probability that users and hackers can access the PBX network and insert malicious software. Mechanisms (hardware and software) that verify the software integrity of PBX system

software and recognize and remove malicious software should be installed and implemented. Use encryption/decryption devices for sensitive voice and data transmissions, if possible.

4.2.3 Sabotage and Other Threats

Protection of telephone equipment is essential in times of war and civil unrest. The threats of disruption of service can include:

1. Denial of Service, externally perpetrated (cable cuts, antenna destruction, and removing power).

2. Denial of Service, internally perpetrated (modifying databases, removing power, and removing circuit packs).

3. Unintentional Congestion (earthquakes and other natural disasters).

4. Intentional Congestion (creating incidents, partially removing equipment from service, and cable cuts).

5. Property Destruction (cable cuts [copper and fiber], equipment destruction [destroying common equipment], disabling climate control equipment, fire, and water damage).

4.3 Natural Threat Sources

Sources of natural threats can be caused by the weather, such as extreme heat, cold, wind; to include storms and flooding. Any of these situations can damage the PBX network and cause loss of service and possibly loss of assets. Backup service can be ensured through the use of a redundant external network system (e.g. route diversity). Provide alternate routes for sensitive and important transmission circuits. An example is to use a cellular/radio or satellite system if the normal landline system is inoperable.

4.4 List of Generic Threats

The following list of threats is not meant to be comprehensive.

1. Masquerade - This is an attempt to gain access to the PBX system by posing as an authorized user. An obvious example is when a hacker, through 'social engineering', is able to obtain an authorized account and password to the system. This can happen via the attendant console, OA&M terminals, or wire-tapping from a cross-connect terminal.

2. Lack of Responsibility - Personnel who are given authority and responsibility

inherent with their position within an organization are responsible for all assets within their purview. The threat lies in the improper performance of duties, such as lack of providing proper accounting of assets and data, and lack of promoting security awareness.

3. Disclosure, Taking, or Unauthorized Use of Documentation - Documentation should be properly managed. Examples are: confirmation of receipt of documents, following proper procedures for discarding outdated documents, proper labeling of documents, and proper transfer of documents.

4. Destruction of Assets - Attention should be given to make sure that deliberate destruction of property is not easily accomplished. Ensure the physical security of the PBX location using logs and alarms for auditing. Make sure supplies and equipment are stored securely.

5. Unauthorized Access to Sensitive Areas - Minimize access to the PBX and ancillary assets. Ensure proper implementation of physical barriers such as security locks and ensure proper validation of terminal access.

6. Compromise of Data (Message or Data Modification) - Data can be in the form of magnetic tapes, disk drives, or system software and documentation (i.e. any information that can be accessed and used for purposes other than what is intended). The threat is in the unauthorized access/alteration/modification of the system database.

7. Denial of Service - These are acts or events that prevent the PBX operating system from functioning in accordance with its intended purpose. An example of this is when an authorized or unauthorized user makes changes to the PBX system configuration wherein resources are disabled or calls are misrouted.

8. Traffic Analysis - This is the action by which a person is able to infer information by monitoring (or eavesdropping) or reviewing CDR records of calls being handled by the PBX. Sample information gathered can be origination/destination of calls, length of call, and frequency of calls.

5.0 Vulnerability Assessment

Threats to telecommunications have increased significantly due primarily to technology. Threats are posed by co-located CPUs, concentrated signalling paths (e.g. STPs), environmental requirements for sensitive electronic elements, and the concentration of communications paths (e.g. fiber optic cables), to name a few. Modifications to call handling have gone from 'hard wired' done locally to electronic modifications done remotely.

The availability of equipment needed to do data modifications and the sophistication and capability of the public to make such changes makes an attack on a communications switch much more plausible. Many threats and associated vulnerabilities have been identified. See Figure 5 (Threat and Vulnerability Relationship).

Vulnerability analysis has to take into consideration the following items.

Threat - any circumstance, condition, or event created/caused by humans within the PBX network environment with the potential to cause harm to the PBX and its ancillary equipment in the form of destruction, disclosure, modification of data, denial of service, and/or fraud and abuse. See Section 4.0 (Threats).

Level of Trust - the concept by which secure systems will control access to and use of the PBX network, encompassing hardware, software, databases, and documentation, such that only properly authorized individuals (users), or processes operating on their behalf, will have access to read/write/modify data pertaining to the PBX network. PBX subscribers also have certain levels of trust to cover the use of switch features and services (e.g. trunk access, DISA access, and long distance calling access).

Points of Vulnerability - it is the point where the PBX network is most vulnerable to attack from threats that controls should be implemented to establish the level of trust. The broad categories of vulnerability points are:

- switch security features,
- switch software and database information,
- switch performance,
- office documentation,
- other (monitoring and technology issues), and
- environmental issues.

Malicious User - this is an individual that intentionally tries to use the PBX switch for unauthorized purposes. Authorized users can be malicious users.

5.1 Switch Security Features

Switch security features define the limitations of users, the service subscribers can use or have access to, and monitor user access and selected user activities. Any attempted unauthorized access or use should be reported via alarms and recorded.

Security features ***may not be implemented or may be poorly implemented***. Poor implementation gives a false sense of security while permitting unauthorized access and use. It also creates insufficient records to determine what has occurred and to assess the damage done or the method of perpetration. Vendors may deliver, test, and turn over switches to the PBX owners with most or all security features disabled. It is the responsibility of the PBX security or network administrator to establish and enforce implementation of the PBX security features.

Unauthorized disruption of services/features is clearly within the capability of the hackers and phrackers. For example, manipulation of the "threshold" setting to allow overload of "origination" messages; creating an event that would require a cold boot or reload of software and databases; disabling of the write protection from the program and data. Other vulnerabilities include disabling of a Signal Transfer Point and its backup, unauthorized changing of translation tables, and penetrating Operations, Administration & Maintenance systems. Disruption of security features can occur when users/subscribers do not properly implement the security protection available on the switch. For example, failure to provide adequate protection to passwords, special access codes or personal identification numbers (PIN) in the open environment of a switch can often be more inadvertent than deliberate. Nevertheless, it can lead directly to the violation of the confidentiality of information/data through the misuse of such switch capabilities as voice mail and electronic mail.

Unauthorized use of services/features has been common since hacking and phracking began. It has been successfully attempted by outsiders as well as insiders. Classic examples include the use of "Blue Boxes", "Red Boxes" or any other of several "boxes" that are used to deceive or circumvent the PBX peripheral modules. There are other unauthorized schemes such as indirect operator services access, call/sell operations, call diverter, remote access fraud, voice and electronic mail fraud, and allowing unauthorized switching to a remote PBX.

Unauthorized access to data/information/software pertains to accessing data/information/software that is normally not accessible to non-users. This includes; switch configuration, routing data, command files, subscriber and/or user profiles, administrator functions, etc. The vulnerability of ***unauthorized manipulation of data, information, or software*** is closely related to, and may be a consequence of, the threat posed by the malicious user. Further, this vulnerability can contribute to the occurrence of other vulnerabilities such as the unauthorized use of services/features, and may be viewed as a natural consequence of an open switch environment.

Improper utilization of security features is closely related to the bypassing of security features. Its primary distinguishing factor may be in the motivation, and is most likely to occur in an environment where there are little or no structured security requirements. As examples, the security audit trail capability of a switch (security log) may be disabled for operational reasons (e.g., increased throughput, additional storage capacity, etc.), password discipline may be ignored to make switch access more convenient, or the implementation of the security feature may be under the control of a switch vendor rather than a switch site (e.g., to facilitate remote diagnostics).

5.2 Switch Software and Databases

Switch software is divided into 3 areas: main (static) program, modifiable switch specific data (e.g. line and trunk information), and dynamic information of calls. The least vulnerable portion of the software is the dynamic information of calls area, since this information is constantly changing due to changes in subscriber call conditions. Disruption or changes in this area of memory will have little impact except to calls directly affected by the area of memory these calls used. This area changes from call to call. A more vulnerable area is where specific switch data is stored. Unauthorized changes to this area may delete resources, change call handling, misroute calls, deny subscriber access, or disable users. The most significant vulnerability is the ability to gain access to the main program and make unauthorized changes via patches, modifications, or insertion of malicious software (e.g. trojan horses, worms, and viruses). An attack on the main program can result in loss of processing, denial of resources, denial of access by users and/or subscribers, theft of program information, modification of the program to allow unauthorized access of valid accounts, or unauthorized use of services or features.

Insufficient hardware/software configuration management that can degrade the availability of the switch operations. It is an issue that can act behind the scenes and impact the ability to manage switch capabilities. Issues of significance include: the integration of PBX software with customer software; the proper allocation of subscriber(s) capabilities; controls over the initial set-up configuration; controls over the changing of components and circuit boards; the nature of and changes to subscriber capabilities and equipment; and the management of the software changes on user controlled switches.

The ***introduction of malicious code to components*** of the PBX is a vulnerability that cannot be ignored. Malicious code will be considered code that can corrupt or subvert the operating system or application program, and prevent the switch from performing as it was intended. Further, malicious code can be introduced into programs intentionally, as is the case with Trojan Horses, or unintentionally as may be the case of a genuine flaw in the program logic or with a programmer error. Once software is corrupted or subverted by malicious code, for whatever reason, it can become a platform for a perpetrator to attempt a variety of attacks, or perhaps more significant to a switch environment, to attack attached switches or networks, subverting them so as to permit the perpetrator to invisibly use them.

Unauthorized user remote access capabilities can be initiated by outsiders using dial-up capability to access a modem located at the switch. This vulnerability can originate through the modem ports which provide remote access to the switch through the I/O port. Remote diagnostics, and remote administration and maintenance are common modem access functions. While there are security procedures and access control features often associated with the use of remote access capabilities, this vulnerability continues to be one of the most common of the external threats.

5.3 Switch Performance

Switch performance is the expectation of the reasonable operation of the PBX during a variety of calling and caller conditions. A properly engineered and installed switch, with features and functions properly implemented should provide reasonable service. It will also have all available features and functions tested and the switch will be designed to handle the expected traffic. Vulnerabilities are created when resources are improperly allocated or are insufficiently provided, or when testing fails to diagnose/find bad hardware or software. This leads to lack of trust that services can be provided.

The vulnerability posed by ***disruption of recovery capabilities*** has received a considerable amount of attention from the vendors in the form of redundancy within components, diagnostic software and parallel functionality. As a result, in order to disrupt services both the primary and redundant capabilities must be affected. Vendor literature identifies areas where potential disruption of recovery capabilities could occur. These includes some of the areas cited above regarding the disruption of services/features, such as the alteration and manipulation of the relationship between the three types of restart (e.g., warm, cold, and reload) and the three categories of memory store for program and/or data (e.g., protected, permanent, and temporary).

The vulnerability posed by a ***failure of switch hardware/software resources*** must also be seriously considered. Availability of information regarding software failures appears to be a function of the magnitude of the impact of that failure. Software failures, which could be of potential significance, but which caused less noticeable consequences have no doubt occurred. Records on PBX failures are not required to be reported.

5.4 Office Documentation

Documentation provides information to the PBX owners, users, and subscribers on the functions, services, maintenance and repair, or PBX site information such as office records. Instructions, guidelines, repair procedures, and information documents should be available. The vulnerability of unauthorized access to documentation is that how the PBX is secured, how to disable or bypass security, how to create false accounts, and how to modify/add/delete data are all described in documents that are necessary for trusted employees to use in the performance of their jobs.

Unauthorized disclosure of switch technology pertains to making information about the operations and functions of a PBX available to individuals who do not have a need-to-know. This type of disclosure has occurred as a result of casually discarding documentation that pertains to operations functions, maintenance and administration of a PBX.

A vulnerability occurs when ***documentation is not properly safeguarded***. Prevention and the safeguarding against disclosure, taking, or unauthorized use of documentation must be implemented by personnel involved in the administration, operation, maintenance, and the use of the PBX network. All personnel should be made aware that this threat, if not countered, could cause serious breach of security, loss of monetary assets, destruction of property, disruption of service, or complete loss of service. Administrators should ensure that all PBX and network documentation, especially system specifications and configuration, be kept in a secure facility. Switch maintenance and operations personnel should ensure that switch documentation (manufacturer's manuals), maintenance logs, Telecommunications Service Requests (TSR), exception reports, equipment trouble and outage logs, and system audit and security logs are kept in secure areas. Attendant console operators should ensure that the system telephone directory information is treated as sensitive information and only 'official' numbers be given out to inquiries. Users should be aware that any paper records kept which contain passwords or access codes of phone features must be safeguarded. Such lapses in documentation control could allow malicious personnel, whether insider or outsider, access to the PBX and the network. By obtaining this documentation, personnel can manipulate the data for their own use. Access to documentation can be used to enable toll fraud, illegal service enhancements, unauthorized monitoring of conversations, or unauthorized disruption of service. The vulnerability posed by the theft of documentation is clearly relevant to the continued availability of switch capabilities.

5.5 Other Switch Related Issues

Evolving technology (hardware and software) is necessary for the telecommunications industry to grow and provide additional features and functions. As the technology continues to evolve, communications functionality provided by the switches could be viewed more and more as a communications application processing on a computer system(s) which happens to be a telephone switch. As such, the argument becomes stronger for incorporating telephone switches into the network security community. The development and implementation of security standards for telephone switches will be a long and arduous task, not so much for the difficulties associated with the technology as it will be for the legal and philosophical issues. In most cases, outside of some basic access control features, security protection is provided in response to specific events which exploited a switch capability. Unauthorized monitoring is a problem that has had much attention and is discussed further in Section 5.5.1.

PBX network administrators should know the basic configuration of the network. Being

familiar with the network will ensure that the administrator is able to study reports from lower levels of maintenance and operations to see if there are any calling patterns developing that are contrary to proper security administration. Such patterns include: excessive use of outgoing trunks (e.g. WATS), excessive number of long distance calls, subscriber access to outside lines when they are not configured for it, or cheaper routes not being used. Look for unusual times and destinations of calls. Administrators will also be able to tell if there is equipment abuse during a study of trouble calls. For example, a subscriber who constantly called in a defective telephone was found, after historical study, to be physically abusing the phone by replacing the handset in an improper manner.

The vulnerability posed by bypassing security features is one with wide ranging implications. It can involve issues that range from the failure to follow correct procedures, to the introduction of new technologies into the switch environment, where those technologies may include adding new security features or the use of COTS operating systems such as UNIX. Effective security features are normally employed in-depth. That is, they appear to a malicious user as a series of obstacles. Often they can be mutually supportive, a characteristic that discourages or may even preclude bypassing. However, the open environment of a digital switch, with limited security features and procedures, has traditionally been no match for a knowledgeable, determined malicious user. For example, a considerable amount of creativity has often been demonstrated by hackers and phrackers when bypassing the protection afforded by passwords, authorization codes, and personal identification numbers. Once obtained, access to such features as Direct Inward System Access, electronic mail and voice mail are routine.

5.5.1 Monitoring Issues

Information transmisson can take many forms - analog, electrical emanations, radio frequency (e.g. microwave and satellite), and digital (plain text or encrypted). Vulnerabilities involve unauthorized monitoring of information being conveyed on the various mediums. Analog message access (voice and data) is most vulnerable to interception since it requires no further processing to monitor the communication. The communication path from the subscriber to the PBX switch matrix is the most vulnerable since this path is usually a hard wired analog connection. This path should be protected to eliminate unauthorized access. Shielding (e.g. TEMPEST) and encryption can be used successfully to eliminate unauthorized monitoring.

Unauthorized monitoring of in-progress calls occurs when the signal carrying the voice/data transmission is being received by someone other than the intended person(s). Any transmission that is sent through the atmosphere can be intercepted. It is also an accepted fact that unencrypted in-progress processes can be intercepted at other points along the transmission route (e.g., frame rooms, telephone closets, etc.). This vulnerability extends to other unintended sources by means such as electrical emanation or the potential for an on-hook telephone instrument to transmit voice signals. In addition

to these classical intercept methodologies, the hackers have found other ways to intrude on in-progress processes by exploiting switch features such as the metallic test access capability.

The ***failure of encryption equipment*** is a potential problem of considerable magnitude that exists across all switch environments. If undetected, it could cause damage with considerably undesirable consequences to both the government and the private sector. Fortunately, most government supplied cryptographic equipment has extensive self-diagnostic capabilities (e.g., Secure Telephone Units III). Normally, the encryption of information/data or voice signals will be transparent to the PBX since all transmissions are digitized whether encrypted or not. The significance of unwittingly transmitting sensitive or classified information/data or voice through a PBX switch cannot be understated.

The vulnerability posed by the ***compromise of cryptographic keys*** is closely related in magnitude to the failure of encryption equipment. Key distribution continues to be a major consideration in the implementation of a successful encryption scheme. Proper procedures must be established and implemented.

5.5.2 Levels of Responsibility

There are multiple levels of responsibilities. A vulnerability occurs when responsibility is not taken seriously. ***Negligence*** is a vulnerability that is more common than one might believe. While individuals might not reveal information/data or switch capabilities by deliberately disclosing it to unauthorized persons, they often disclose it through carelessness or preventable accidents. Responsibility starts with the management level and extends all the way to the PBX technician and PBX subscribers. Managers should be aware that they are responsible not only for the proper and efficient running of their PBX network but also for making sure that security awareness and training is implemented. Proper training of personnel makes people aware of the threats to their system and allows implementation of countermeasures against these threats. There must be a person whose major responsibility is PBX network security.

Switch maintenance and operations personnel should be aware of their responsibilities. Their primary responsibility is to ensure the proper operation of the switch network through proper and timely maintenance. Once this is done, their secondary responsibility is to ensure that the switch network is secure from malicious tampering of both hardware and software by either authorized users doing unauthorized things or unauthorized external personnel. Possible entry points for malicious activity should be monitored. This could be the modem used by the remote technician to access the switch database and maintenance modules. This could be system terminals used for a purpose that they were not intended. Maintenance and operations personnel are also responsible for monitoring pedestrian traffic near the switch and making sure that only authorized personnel are allowed access to the switch equipment rooms. They are responsible for making sure

that switch facilities access is given only to authorized personnel and kept locked when the facility are not staffed. They are responsible for overseeing the equipment used by the subscribers, such as telephones and data terminals, and ensuring that there is no fraud or abuse of such equipment.

Attendant console operators have the responsibility of ensuring that only authorized subscribers are allowed access to selected features of the network. Access includes such features as long distance calling, conference calls, or executive override of a pre-existing conversation. They are also responsible for making sure that no conversation is being eavesdropped on using attendant console features.

PBX switch subscribers have the primary responsibility of using the services and features of the switch they are allowed access to. Subscriber features and services could be call-waiting, ring-again, or last number redial. It is also the subscriber's responsibility to ensure that he is aware of the proper procedures for using his assigned features and services. Improper use or misuse of services and features can degrade the PBX switch integrity. Certain features and services require access codes. Such access codes must be protected and not given to unauthorized personnel. An example of a feature or service which may require an access code is long distance dialing. The access code gives the switch administrator a way of monitoring the amount of toll calls being made by individual subscribers. If the access codes are compromised, then toll calls may be made fraudulently.

5.5.3 Evolving Technology

Technology, competition, and customer demand act in concert to pose a vulnerability to the integrity of the switch environment primarily when they are not being offset by the implementation of additional security protection. If the customer was able to write his/her own code (or manufacture their own hardware), the features needed would be under control of the customer. The customer could control the cost, feature content, and operation of the feature. Vulnerabilities exist when the customer fails to control the environment of the software/hardware development, fails to verify feature interactions with other switches or switch functions, or the customer provided computer running the feature is either compromised or fails. Vendors and owners will have to work together to assure the new architecture are successfully implemented without compromising security or creating unresolved vulnerabilities. New software platforms must have sufficient security capabilities established to allow the PBX owner to control access and use of the PBX and the services provided. Care must be exercised to assure that existing controls are not compromised when migrating from one system/architecture to another. Technology can be disclosed by former negligent, disgruntled employees who have knowledge of PBX capabilities and functions. This information can be used to circumvent, modify, or disable security features. It can also be used to gather/modify switch database information. It is not unusual for descriptions of PBX functionality, features and capabilities to be published in hacker and phracker publications.

Government regulation and legislation may unwittingly create vulnerabilities by their continuing quest to ensure an equal opportunity for all vendors to participate in the communications market place. Under this concept the availability of software to outsiders (those who did not develop it) may be required by government regulation to maintain competitiveness among providers. While this effort may raise the level of fairness, it may also lower the probability of maintaining the integrity of software that cannot be protected as proprietary. Information about the software/hardware architecture is made available under the 'Freedom of Information Act' to unauthorized users.

There are also vulnerabilities created by ***evolving telecommunications architecture.*** Current telecommunications capabilities are provided by vendor supplied software. The vendor assures the functionality, compatibility with other features and functions, and documents the capability. To change/add features takes time, may require a hardware and/or software upgrade, and is provided on a per switch basis. Some features require data common to all switches, but must be 'copied' into each switch with that feature (e.g. when a new area code is added, all switches must be upgraded to allow any caller to be routed to the new destination). By moving this data to a common database such as a Service Control Point (SCP), all switches have access to the same data and if the data has to be changed, it only has to be done in one place. The vulnerability is that if access to the SCP is denied, the switch will be unable to complete call traffic.

The vulnerability posed by ***insufficient security in switch design*** is a programmatic vulnerability that effects every aspect of the switch. The relevance of this vulnerability is manifested in the switch design itself. That is, switches are designed to be user friendly and economical. The same design features which produce these characteristics also make them easy to attack.

5.6 Environmental Issues

Newer PBXs using electronic components are much more ***vulnerable to environmental changes***. This is not to say short term violations and variations would not be tolerated, but long term events may cause serious problems. The environmental conditions on a building includes temperature and humidity, power, physical access, drainage, and high wind conditions. Temperature and humidity, power controls, drainage, and high wind controls help protect the PBX from being destroyed by natural events such as flooding, fires, wind and rain damage, and power surges or extended power loss.

Physical access control prevents unauthorized access to the PBX facility. Controlling access limits: compromise of documentation, unauthorized access to the switch, and destruction of property and acts of sabotage. A ***vulnerability occurs when assets*** (e.g. switch rooms, telephone cross-connect closets, telephone stations, and Public Switch Telephone Network (PSTN) to PBX demarcation points) ***are not properly secured***. Procedures and guidelines for the prevention of unauthorized entry or use of such facilities and equipment should be implemented by any personnel involved in the

administration, operation, or maintenance, and the use of the PBX network. Physical access to switch components, telephone closets, utility rooms, and cable runs must be constrained by adequate physical protection which precludes unauthorized access (e.g., doors, locks, cipher locks, conduit, alarms, positive identification and verification systems). Restrict access to equipment use to authorized personnel. Minimize sharing of telephone closets and other support facilities with non-PBX equipment or from other telephone systems that are not part of your own and, therefore, not under your control. The total process of identifying, controlling, and eliminating or minimizing events that may affect system resources includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review.

The vulnerability posed by ***vandalism and/or civil disorder*** cannot be ignored when considering vulnerability to the availability of switch services. If one considers the hacking and phracking incidents identified in this analysis as vandalism, then it is clear that the vulnerability of vandalism has been active. Hackers have accessed company property using fake ID's. A serious breach of organizational security, loss of monetary assets, destruction of property, disruption of service, or complete loss of service are direct results of this type of vulnerability that all personnel should be made aware of. There are people who, for reasons known only to themselves, will try to infiltrate these telecommunication centers and cause damage to the network.

6.0 Basic Telephone Switch System Security Capabilities

This section covers the security capabilities of the PBX switch. The main goal is to prevent unauthorized use, unauthorized access, and unauthorized manipulation of the switch database, operating software, routing translations, and configuration. There is a need to provide secure telephone service to the organization and protect the telephone equipment investments of the organization while maintaining an environment for the operations, administration, and maintenance personnel. Security measures are required full time to combat internal or external threats that are deliberate or accidental. See Figure 8 (Generic PBX Functionality Overview).

1. Office Images or Backups - The switch database (configuration information, journal files, audit files, and log reports) should be downloaded or backed up at least daily. Backups will ensure that when there is a switch crash, there is a good, clean source from which to bring the system up with minimal or no loss of data. Backups should be written to two separate and distinct devices, either hard disk drives or magnetic tape drives. This way, if one device fails there is a backup media to ensure continued backups. Keep and store magnetic tape backups in a secure area, not co-located with the switch so that in the event of switch destruction (e..g. fire) another switch can be brought up using the back-up data.

2. Call Detail Recording - These records can be used to determine unauthorized use of the PBX. These records may be used internally to allocate funds to departments for telephone usage by that department. Calls with unusual times (e.g. after business hours) or unusual destinations (e.g. calling to where a location the company does not do business) may indicate unauthorized access and/or use has occurred. These records should be kept for use in developing patterns of use/abuse. All records containing details of PBX call activities should be stored in a secure place.

3. Hardcopies - Hardcopies (paper product) should be made of routing tables, switch parameters database, trunk records, and line records. This information is contained in the office backup. In the event that there is a switch failure and the switch is brought up using the office backup, information in the switch can be compared to these hardcopies to assure database integrity. Keep and store hardcopies in a secure area.

4. Dial-up Access to the PBX - Guard against unauthorized connections through the dial-up access ports to the PBX. All dial-up access should be pre-arranged and/or scheduled for PBX administrator positive control. This control might consist of manual answer on the modem, manual activation of the port in the PBX, or a dial-back feature.

5. Login Control - The login control feature of the PBX should be used to assist in controlling the use of the direct connect and dial up ports to the switch. Such ports are typically used by the operation, administration, and maintenance terminals. This feature allows the automatic disabling of the port after disconnection by the user, as well as limiting the number of times and attempts at logging into an enabled port. This is a valuable enhancement to switch security and will reduce the possibility of ports being left in an vulnerable state.

6. Man/Machine Access - Operation, administration, and maintenance terminals should be logged out when not in use or unattended. User passwords should be changed regularly. Local procedures should be implemented and followed for the disposal of printout paper and other obsolete documentation.

7. Input Command Screening - All PBX commands should be given a classification to restrict a user's command set to the set of commands which will permit personnel to perform specific job functions. This can prevent accidental or intentional database changes by unauthorized personnel. Such classification should be controlled by the PBX security administrator.

8. Switch Security Features - Any security features of the switch, such as audit trails, history reports, alarms, and exception reports should be activated. These reporting and alarm systems will identify many man/machine activities which may be fraudulent or malicious.

9. Remote Maintenance - Switch manufacturer personnel access should be controlled. All request for remote maintenance should be authenticated. All remote maintenance should be recorded in an activity log and should include the following information: name of remote maintenance personnel, on-site personnel allowing access to remote personnel, date and time of login, purpose of login, and time of logout.

7.0 PBX System Administrator

PBX system administration refers to the duties and responsibilities associated with the operations, maintenance, and monitoring of a PBX. To ensure the successful operation of the PBX, the PBX system administrator is responsible for accomplishing the following duties:

1. Initialize the system.
2. Manage the system's voice terminals, data terminals, and associated features.
3. Ensure daily system backups are accomplished.
4. Monitor system performance.
5. Maintain adequate system security.

7.1 Know your PBX

Become familiar with the PBX and all adjunct system capabilities. First and foremost, the administrator must understand most, if not all, capabilities of the PBX and its operations. The administrator should be familiar with the operations that affect switch security. Examples of such operations are:

1. Logon account names and passwords used by the vendor/manufacturer. Any default passwords should be changed.
2. Station call detail recordings.
3. Time of day (day of week) restrictions.
4. Security reports that are available.
5. Facility restriction levels which should be implemented.
6. Remote access which must be controlled.
7. Class of service restrictions.

While there is no product that totally prevents unauthorized invasion, damage, or use of the PBX assets, switch manufacturers have designed many features to help administrators minimize the risks of loss from unauthorized access or by toll fraud. PBX system administrators must select and implement those features that best meet their

needs while recognizing the trade-offs between security, convenience, flexibility, and cost-effectiveness.

7.2 Monitor PBX Options and Settings

Periodically, monitor all PBX and adjunct system options and settings. Continual system monitoring helps identify changing call patterns, switch function and feature utilization, and possible security issues. Timely modifications can be made to secure both call routing and calling privileges to help safeguard against unauthorized modification and use. The PBX provides call detail reports to assist the administrator in determining if the system is being used as intended. When the PBX is first installed, custom ordered features were loaded into the switch, in addition to the basic set of features. If you do not have the documentation detailing such features, then you should work with the PBX account team and the manufacturer to try and obtain this documentation to ensure proper application, while ensuring the information is retained and safeguarded. Monitor system parameters and settings that have an impact on the security of the PBX. A periodic backup and verification of the system memory should be done to detect illegal tampering and monitoring of system memory for changes. Determine the normal settings for the PBX and periodically confirm that these settings have not been changed.

7.3 Passwords Management

Set passwords requirements to conform to organizational security policies. Passwords must be used and must fulfill established organizational requirements. Change passwords periodically and ensure that passwords are of sufficient length to hinder hackers. Passwords should be safeguarded and not seen by the system administrator or other personnel. Default passwords should be changed. Non-english words (e.g. "XPQ6@" OR "P9>#DD@*") should be used as passwords. If non-alphanumeric characters are valid entries, use of special characters is preferred.

7.4 Review Telephone Bills

Ensure that telephone bills and call detail reports are reviewed for fraud and abuse. Review monthly bills from the phone company for calls that are out of the ordinary. Numerous calls to a 900 number may indicate telephone system abuse, while high volumes of 800 number calls may be indicative of fraudulent activities. When reviewing these records, look for the following indicators of fraud or attempted fraud:

1. Numerous inbound calls of a very short duration which often indicate hackers are attempting to discover access codes

2. Outbound calls of long duration

3. High volume of calls during off-peak hours

4. High volume of calls to locations not typically called by the organization

5. An inordinately high volume of calls to any location

6. A constant busy signal on inbound 800 circuits

Call Detail Recording (CDR) provides detailed information concerning an incoming or outgoing call. CDR is administered by the system administrator. Call detail records are generated during call processing and are sent to the CDR output device. This information can be used to facilitate cost allocation, analyze traffic, and detect unauthorized calls. The originally dialed extension number on an incoming call, or the originators extension number on an outgoing call is always recorded for CDR even if the call is transferred to another voice extension. Other details in the CDR include: facility restriction levels, called/calling (trunk) number, type of trunk group used for the call, time of call completion, call duration, and inter-exchange carrier used.

7.5 Educate Fellow Employees about PBX Fraud

All users and subscribers should be made aware of the vulnerabilities of a PBX and their specific responsibilities in protecting the PBX and other adjunct systems.

7.6 Activate PBX System Security Features

All PBXs have built in security features. It is up to the system administrator to activate and enforce them. This section will discuss some standard switch security features.

7.6.1 Set Time of Day Restrictions

In safeguarding the PBX, it may be desirable to limit access to PBX services outside of normal business hours. This feature is normally used to take advantage of lower calling rates during certain times of the day and week.

7.6.2 User Access

Restrict access to only those users with an operational requirement. User access is controlled through class of service restrictions and facility restriction levels. Review the necessity for access to the extensions associated with the following functions:

1. Administrative or maintenance access ports to the PBX or adjunct processors

2. Automated attendant access ports (e.g. VM or ACD)

3. Extensions assigned to modem pools

7.6.3 Prohibit or Restrict DISA Use

Prohibit or restrict the use of Direct Inward System Access (DISA). DISA (sometimes referred to as Remote Access) is a feature that allows authorized subscribers to make long distance calls through the PBX. Typically, the subscriber dials a toll free or local number (terminated within the PBX) from a remote location which is auto-answered by the PBX. The PBX will then prompt the subscribers (either via a second dial tone or voice announcements) to dial the DISA authorization code. Once access is provided, the subscriber will then be able to use PBX features consistent with the authorization codes as if they were directly connected to the PBX. Remote access should only be allowed for official and authorized purposes.

7.6.4 Restrict Call Transfer Capabilities

Restrict call transfer capability for automated attendant system to within the PBX. An automated attendant system (often a voice mail feature or Automatic Call Distributor) provides unattended processing of incoming telephone calls. PBX Administrators must be aware that although these systems can greatly reduce the number of attendant-processed calls, they also offer an avenue for PBX fraud. If a hacker is able to gain access to outgoing PBX services, they may originate long distance calls that will be billable to the organization.

7.6.5 Limit Telephone Service

Limit telephone service functions and features to those that are required by the subscriber. The type of calls any station is allowed to make is controlled by the facility restriction levels and the class of service features that are assigned to that terminal. Restrictions and service features control functions such as:

1. Station and trunk group access

2. Network calling privileges

3. Calling party restrictions - denial of service to certain area codes and selected end offices, denial of direct outward dialing to the Public Switched Telephone Network, and toll restrictions

4. Called party restrictions - deny subscribers at specified telephone stations from receiving Public Switched Telephone Network calls, attendant-originated and attendant-extended calls

7.6.6 Make Subscribers Aware of Their Responsibility

Ensure the subscribers are aware of their telephone system security responsibilities. The

PBX system administrator is responsible for ensuring that subscribers of the PBX are aware of the PBX features (e.g. voice mail) and aware of the following responsibilities:

1. Use telephones and their services for official business purposes only.

2. Be alert to social engineering scams, be suspicious of callers asking you for passwords or access codes for any purpose.

3. Notify the PBX Security Administrator if you suspect telephone services are being used for fraudulent purposes.

4. Keep all system passwords and access codes secret.

5. Keep long distance call access codes secret.

6. Ensure that your telephone services authorization code is as long as possible.

7. Change telephone services authorization codes frequently.

8. Review call detail records for unauthorized use.

7.6.7 Maintain Good Configuration Management Records and System Backups

The PBX's database change history feature allows the PBX administrator to view or print a history report of the most recent administration and maintenance changes. The PBX administrator should print a copy of this file periodically for safekeeping. The administrator should keep at least a few months history reports on file. System backups should also be done daily and the administrator should keep multiple backups for safekeeping.

8.0 Figures

Figure 1 Typical PBX Network Connections

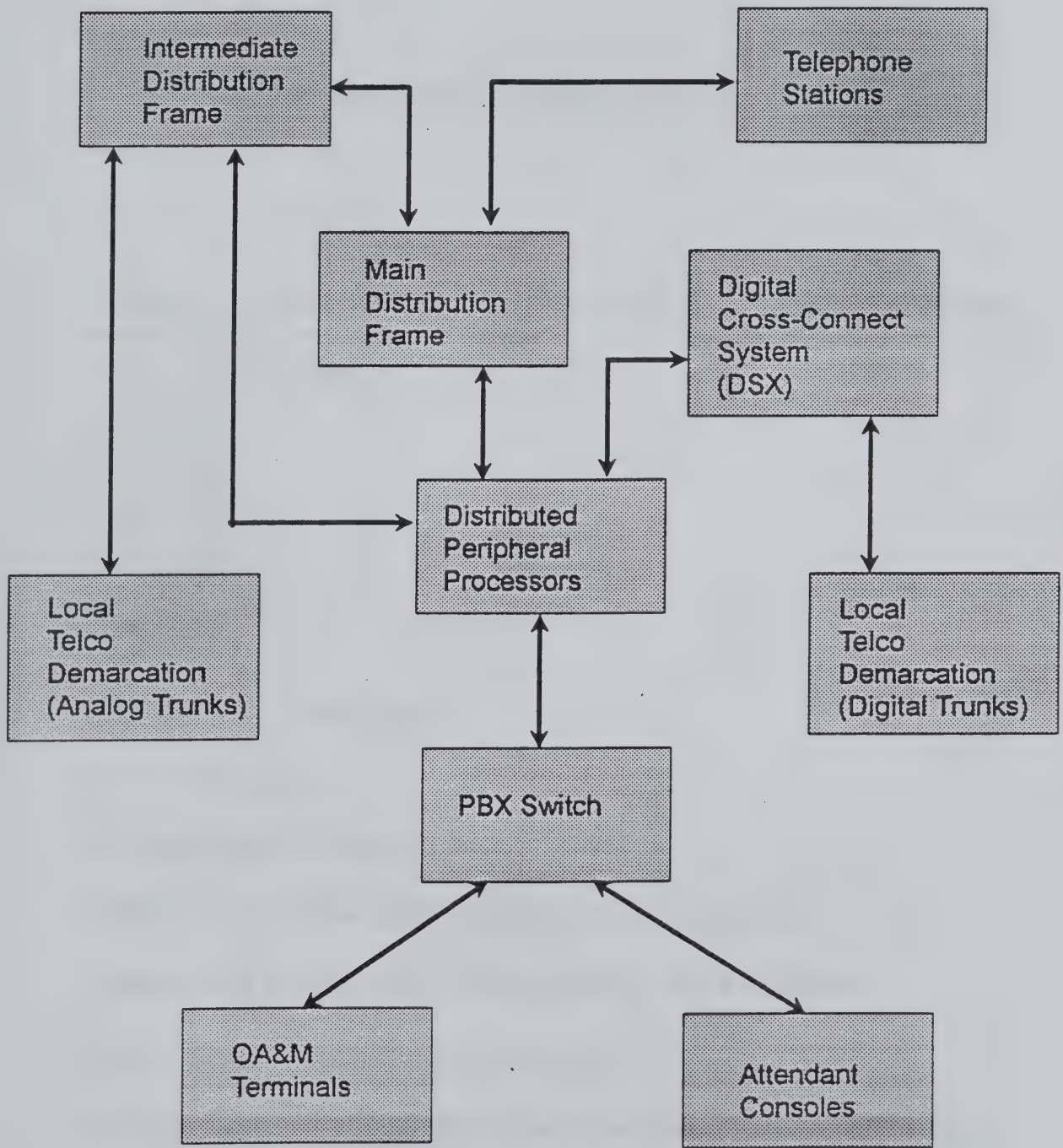


Figure 2 North American Numbering Plan

North American Numbering Plan

Prefix	Area Code	Office Code	Station Number
1	N [0/1] X	NXX	XXXX

LEGEND:

N = any digit 2 through 9

0 / 1 = Digit 0 or 1

X = Any digit 0 through 9

Prefix = Intra/Inter LATA Calls in North America

Numbering Plan Area = Geographical Area Access

Office Code = Individual Exchange

Station Number = Specific Station within a Given Office Code

Figure 3 Modular Switch Components

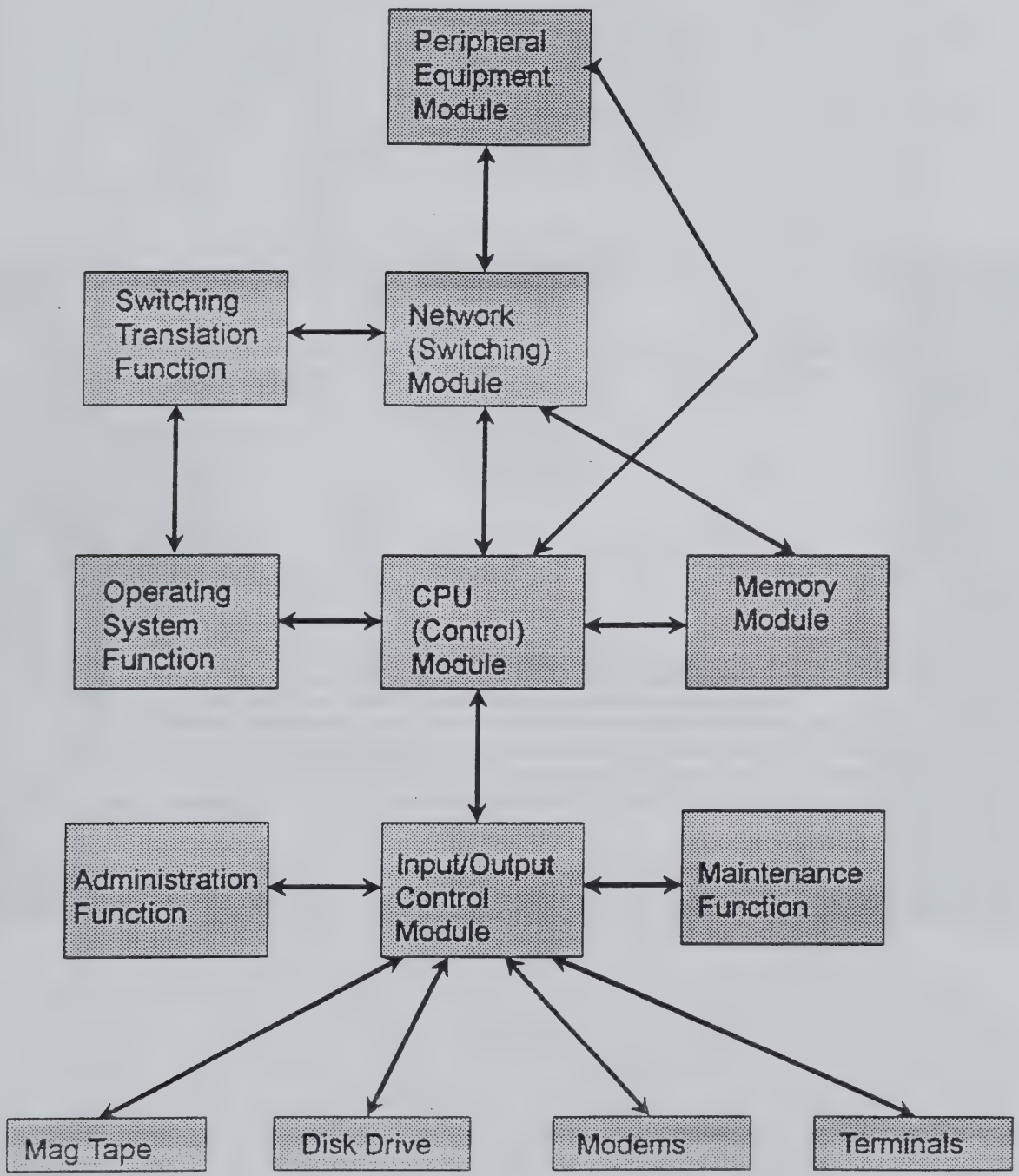


Figure 4 Common Channel Signalling

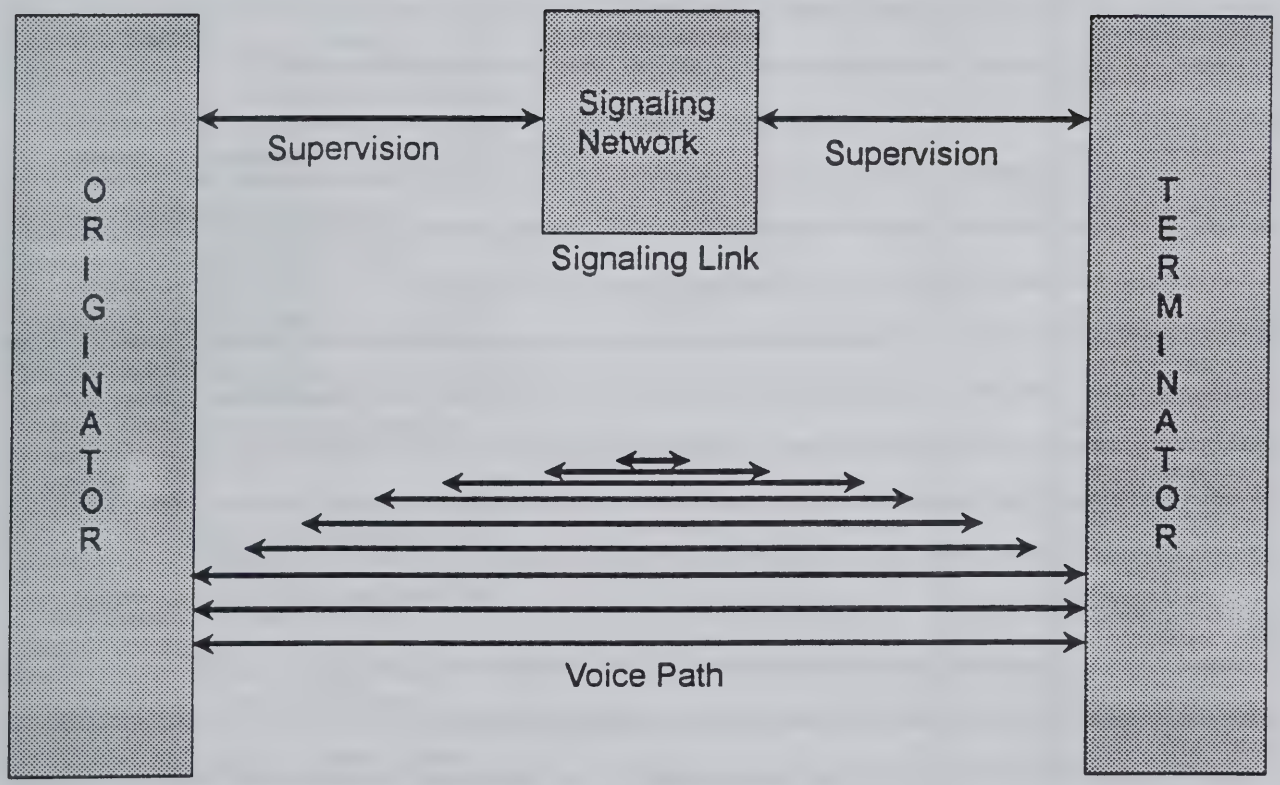


Figure 5 Threat and Vulnerability Pairing

HUMAN (INTRUDER OR HACKER)	CONFID	INTEG	AVAIL
Malicious user/subscriber	s	p	-
Introduction of malicious code to component	-	p	s
Theft of equipment/software/documentation	p	s	p
Sabotage hardware/software/firmware	-	s	p
Bypassing security features	s	p	s
Improper utilization of security features	s	p	s
Unauthorized access to data/information/software	p	s	-
Unauthorized manipulation of data/information/software	s	s	p
Unauthorized erasure of database files	-	s	p
Misrouting of user/subscriber processes	s	s	p
Unauthorized use of services and/or features	-	p	s
Unauthorized disruption of services and/or features	-	s	p
Unauthorized monitoring of in progress calls	p	s	-
Vandalism	-	s	p
Unauthorized disclosure of switch technology	p	p	s
Unauthorized use of remote access capabilities	-	s	p
Disruption of recovery capabilities	-	s	p
Insufficient design of security into switch	s	p	s
"Open" software design, development, testing	-	p	s
Failure to identify and diagnose errors	-	s	p
Insufficient security administration/implementation	s	s	p
Improper use of physical barriers	p	p	p
KEY:			
(-) = negligible			
(s) = secondary			
(p) = primary			

Figure 5 (continuation)

HUMAN (EMPLOYEE OR HACKER)	CONFID	INTEG	AVAIL
Lack of responsibility	-	s	p
Negligence	p	p	p
Inadvertent access to components/services/features	-	p	s
Inadvertent destruction of capabilities	-	s	p
Failure of switch hardware/software resources	-	s	p
Inadvertent disruption of security features	s	p	p
Insufficient contigency planning	-	-	p
Insufficient software/hardware configuration management	-	s	p
Technology, competition, customer demands (open system architecture	-	s	p
Government regulations/legislations	-	p	s
PHYSICAL (NATURAL AND UNNATURAL)			
Temperature/humidity fluctuations	-	-	p
Heating and cooling failures	-	-	p
Inadequate building construction and repairs	-	-	p
Failure of encryption equipment	p	s	-
Compromise of crypto keys	p	s	-
TEMPEST	p	-	-
Fire (including smoke damage)	-	-	p
Weather (and all its effects)	-	-	p
Electrical (lightning, outages, fluctuations)	-	-	p
KEY:			
(-) = negligible			
(s) = secondary			
(p) = primary			

Figure 6 Basic Threat Evaluation Process

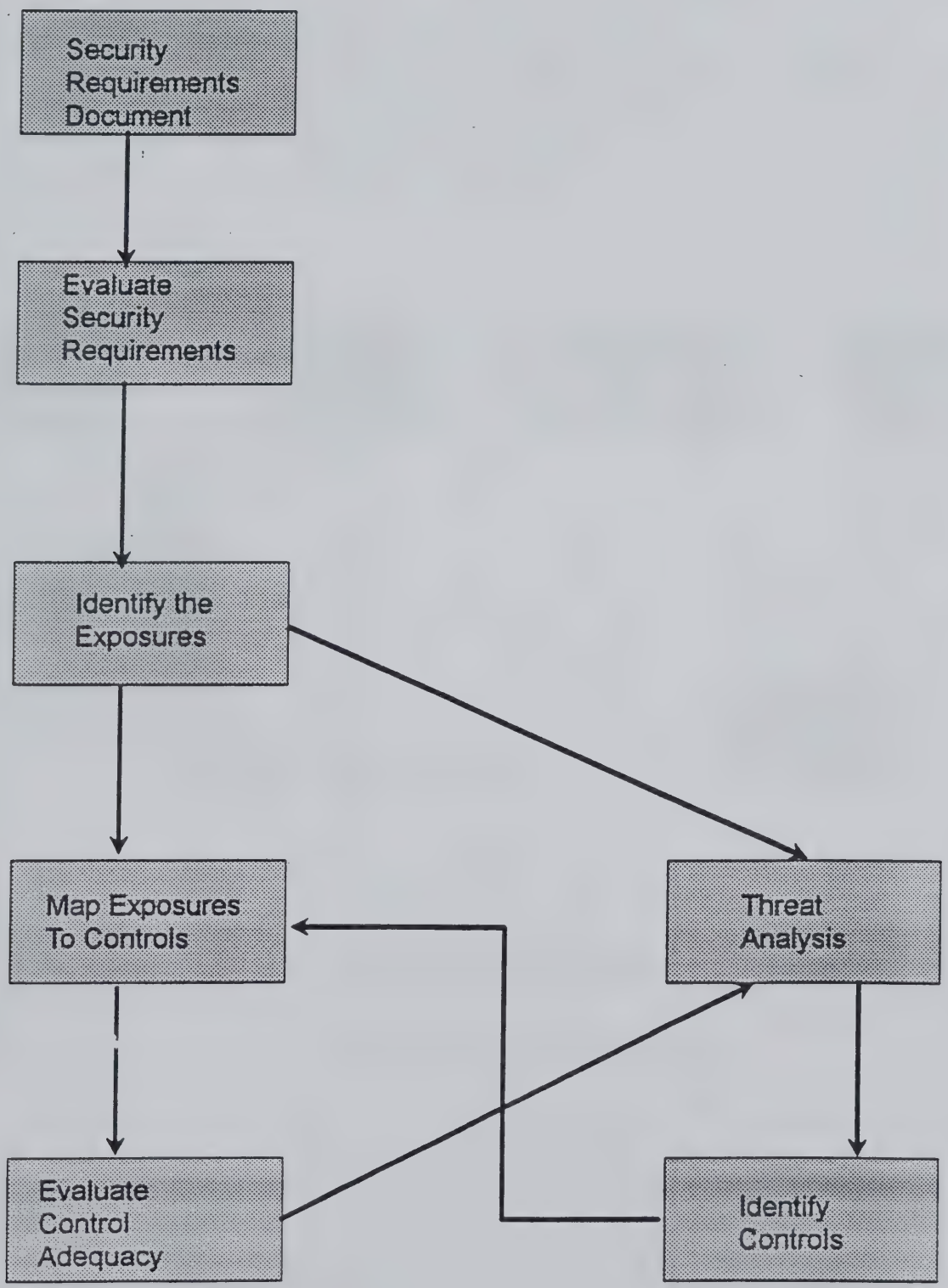


Figure 7 Modification of the FIPS 102: Certification Process

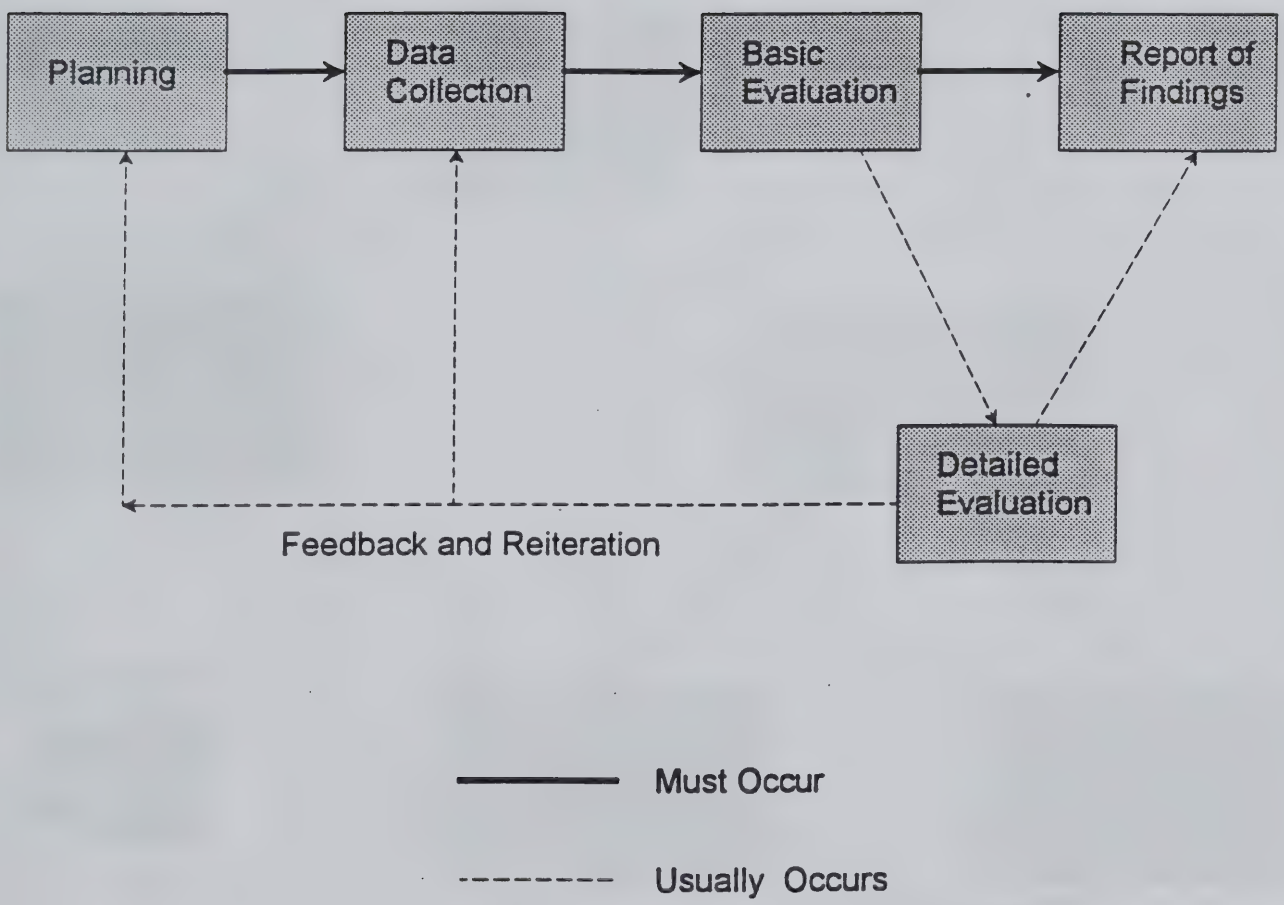


Figure 8 Generic PBX Functionality Overview

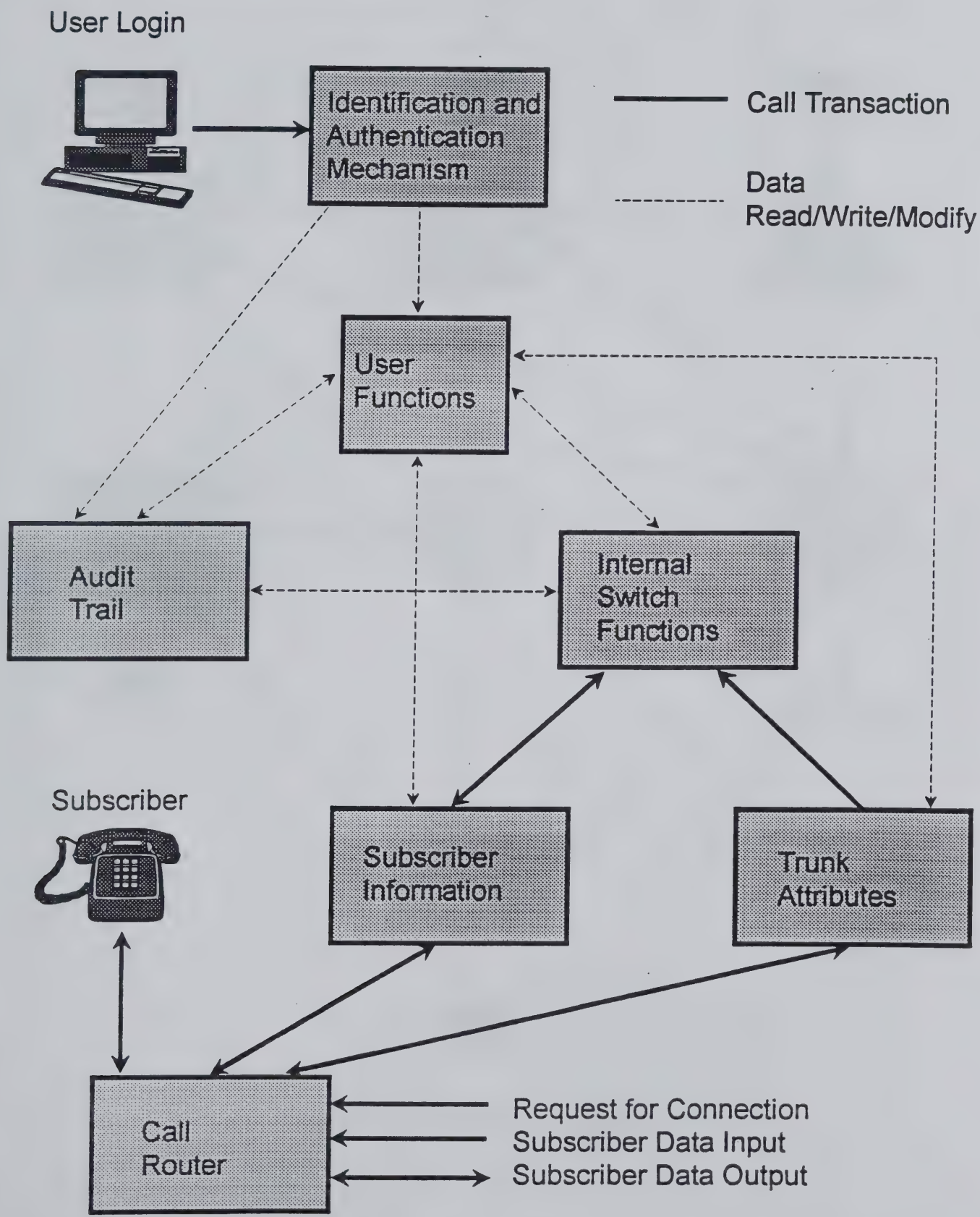


Figure 9 PBX as Part of the PSN

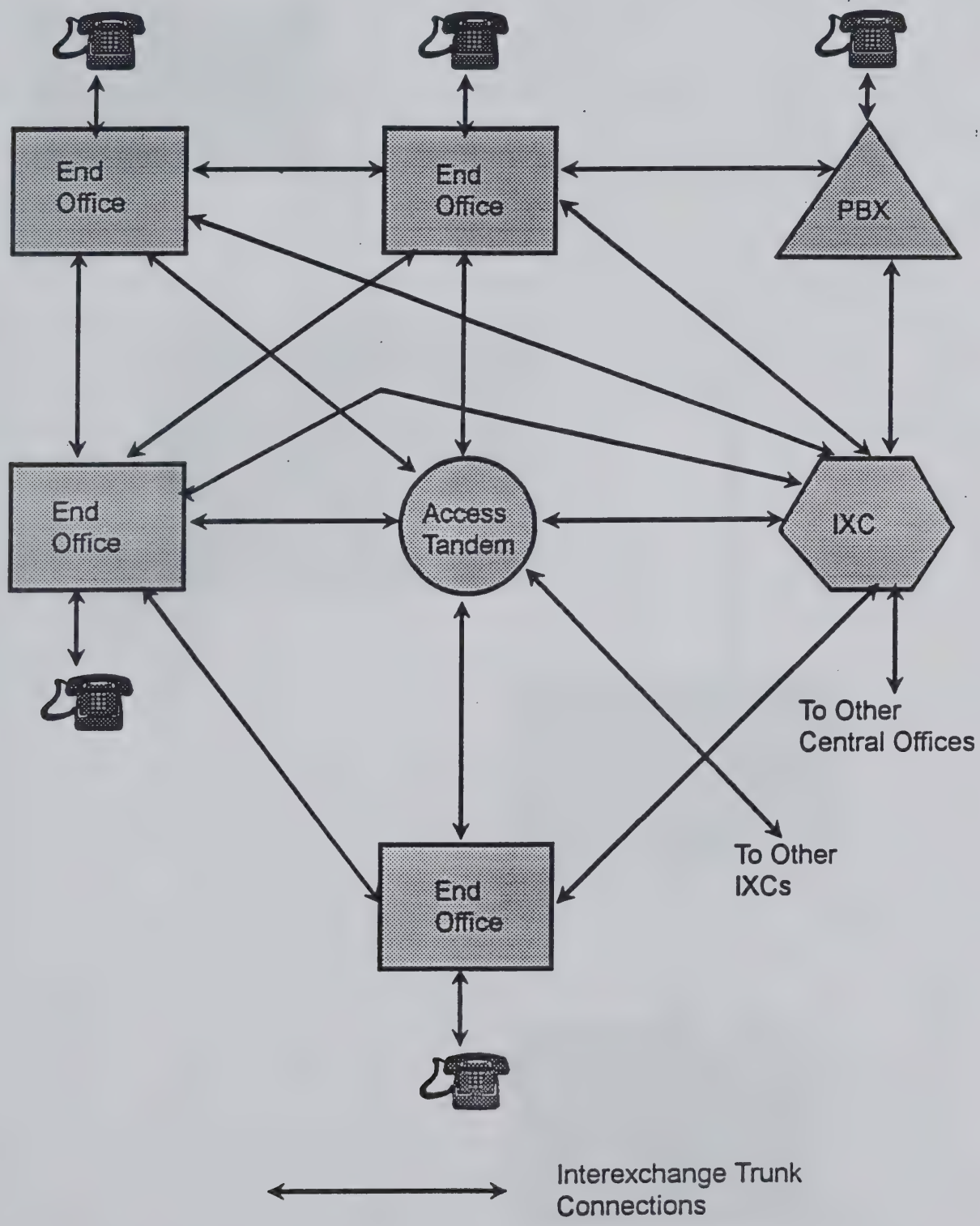
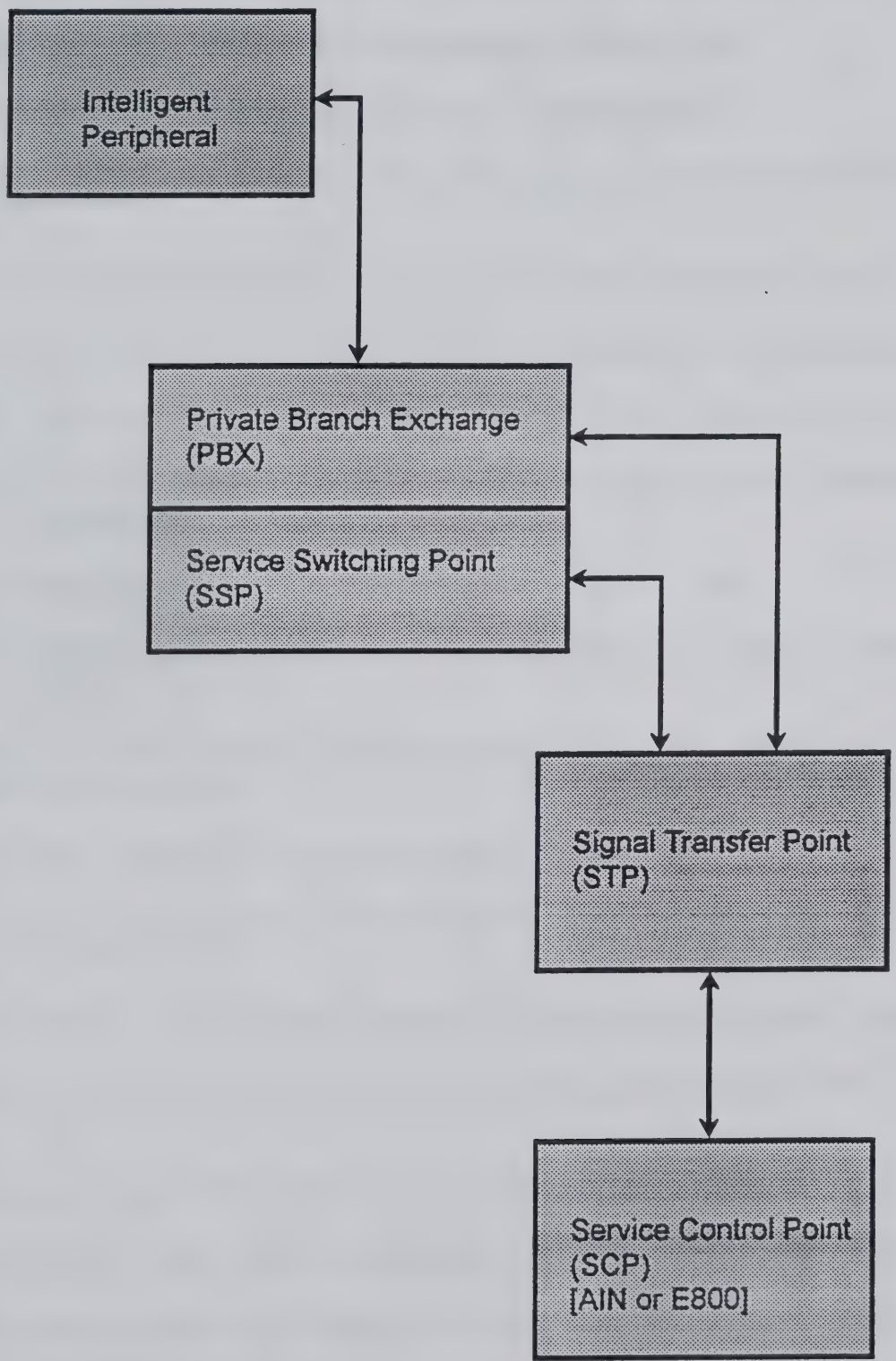


Figure 10 PBX as Part of a CCS7 Network



9.0 References

GAO/RCED-93-79FS Interruptions of Telephone Service; March 1993

Digital Telephony, 2nd Edition; John Bellamy; copyright 1991

Reports on Information Security; Data Pro; copyright 1989

NCSC-TG-005 (Ver 1); Trusted Network Interpretation; National Computer Security Center

DOD 5200.28-STD; DOD Trusted Computer System Evaluation Criteria

FIPS 102; Guideline for Computer Security Certification and Accreditation

NIST Draft Technical Report; Telecommunication Security Guideline; May 17, 1993

Meridian SL-100 Resident Maintenance and Operations Standards Handbook; Northern Telecom Inc.

"For Whom The Bell Tolls"; Forbes Magazine; August 3, 1992

"Phone-Service Theft at Companies Surges"; Business Day; New York Times; August 28, 1992

"Paying the Bill for Hostile Technology: PBX Fraud in 1991"; ISP News; September/October 1991

"Terminal Delinquents"; Esquire Magazine; December 1990

"GAO Says Network Outages Hurt National Productivity"; Telephony Magazine, March 22, 1993

"AT&T Gaining Ground in Battle Against Toll Fraud"; Network World, February 8, 1993

"MCI Intros Progressive Toll Fraud Prevention Program"; Network World, February 15, 1993

"Monitoring Service Thwarts Toll Hacker"; Network World, March 1, 1993

"Surveys Says Large Users Hit Hard by Toll Fraud Losses"; Network World; April 5, 1993

"User Loses to AT&T in Toll-Fraud Case"; Communications Week, March 22, 1993

10.0 Abbreviations and Glossary

10.1 Abbreviations

AIN - Advanced Intelligent Network

BLV - Busy Line Verification

CCS - Common Channel Signalling

CDR - Call Detail Recording

CPU - Central Processing Unit

COTS - Commercial-off-the-Shelf

DID - Direct in Dial

DOD- Direct out Dial

DISA - Direct Inward System Access

DPP - Distributed Peripheral Processor

DSX - Digital Cross-Connect

DTMF - Dual Tone Multi-Frequency

IDF - Intermediate Distribution Frame

ISDN - Integrated Services Digital Network

IP - Intelligent Peripheral

IXC - Interexchange Carrier

MDF - Main Distribution Frame

NAC&I - National Agency Check and Inquiry

NANP - North American Numbering Plan

OA&M - Operations, Administration, and Maintenance

PBX - Private Branch Exchange

POP - Point of Presence

PROM - Programmable Read Only Memory

PSTN - Public Switched Telecommunications Network

RAM - Random Access Memory

ROM - Read Only Memory

SMDR - Station Message Detail Recording

SCAI - Subscriber Controlled Access Interface

SCP - Service Control Point

SSP - Service Switching Point

STP - Signal Transfer Point

TSR - Telecommunications Service Requests

WATS - Wide Area Telephone Service

10.2 Glossary of Telecommunications and Security Terminologies

Acceptance Inspection - The final inspection to determine whether or not a facility or system meets the specified technical and performance standards, Note: This inspection is held immediately after facility and software testing and is the basis for commissioning or accepting the information system.

Access - A specific type of interaction between a subject and an object that results in the flow of information from one to the other.

Access Control - The process of limiting access to the resources of a system only to authorized programs, process, or other systems (in a network). Synonymous with controlled access and limited access.

Access Control Mechanism - Hardware or software features, operating procedures, management procedures, and various combinations of these designed to detect and prevent unauthorized access and to permit authorized access in an automated system.

Access Level - The hierarchical portion of the security level used to identify the sensitivity of data and the clearance or authorization of user. Note: The access level, in conjunction with the nonhierarchial categories, forms the sensitivity label of an object. See category, security level, and sensitivity label.

Access List - A list of users, programs, and/or processes and the specifications of access categories to which each is assigned.

Access Period - A segment of time, generally expressed on a daily or weekly basis, during which access rights prevail.

Access Port - A logical or physical identifier that a computer used to distinguish different terminal input/output data streams.

Access Type - The nature of an access right to particular device, program, or file(e.g., read, write, execute, append, modify, delete, or create).

Accountability - The property that enables activities on a system to be traced to individuals who may then be held responsible for their actions.

Address - (Sometimes referred to as "called number.") That group of digits which makes up a telephone number. For example, an address may consist of area code, central office, and line number.

Administrative Security - The management constraints and supplemental controls

established to provide an acceptable level of protection for data. Synonymous with procedural security.

ANI (Automatic Number Identification) - Automatic equipment located at a local or toll dial central office used to identify the calling number in customer-dialed toll calls. The identity of the calling number is transmitted to CAMA by means of multifrequency pulses that are sent over the same trunk after dial pulsing has taken place.

Attack - The act of trying to bypass security controls on a system. An attack may be active, resulting in the alteration of data; or passive, resulting in the release of data. Note: The fact that an attack is made does not necessarily mean that it will succeed. The degree of success depends on the vulnerability of the system or activity and the effectiveness of existing countermeasures.

Audit Trail - A chronological record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results.

Authenticate - (1)To verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system. (2)To verify the integrity of data that have been stored, transmitted or otherwise exposed to possible unauthorized modification.

Automated Security Monitoring - The use of automated procedures to ensure that security controls are not circumvented.

Back Door - Synonymous with trap door.

Backup Plan - Synonymous with contingency plan.

Browsing - The act of searching through storage to locate or acquire information without necessarily knowing of the existence or the format of the information being sought.

Call Back - A procedure for identifying a remote terminal. In a call back, the host system disconnects the caller and then dials the authorized telephone number of the remote terminal to reestablish the connection. Synonymous with dial back.

CCIS (Common Channel Interoffice Signalling) - A type of signalling system in which all of the signalling information, including supervision and address signals, for a number of interoffice trunks is encoded and transmitted over a separate signalling link by means of time division multiplexing.

Common Channel Signalling (CCS) - A signalling method in which a single channel conveys, by the means of labeled messages, signalling information relating to a multiplicity of circuits or calls and other information, such as that used for network management.

Class of Service - The categorization of telephone subscribers according to specific type of telephone usage. Telephone service distinctions include, for example, rate differences between individual and party lines, flat rate and message rate, and restricted and extended area service.

Communications Security (COMSEC) - Unauthorized persons information derived from telecommunications of the U.S. Government concerning national security, and to ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, emission security, and physical security of communications security material and information.

Compromise - A violation of the security policy of a system such that unauthorized disclosure of sensitive information may have occurred.

Computer Fraud - Misrepresentation, alteration or disclosure of data in order to obtain something of value (usually for monetary gain). A computer system must have been involved in the perpetration or coverup of the act or series of acts. A computer system might have been involved through improper manipulation of input data; output or results; applications programs; data files; computer operations; communications; or computer hardware, systems software, or firmware.

Computer Security Subsystem - A device designed to provide limited computer security features in a larger system environment.

Configuration Control - The process of controlling modifications to the system's hardware, firmware, software, and documentation that provided sufficient assurance that the system is protected against the introduction of improper modifications prior to, during, and after system implementation. Compare configuration management.

Configuration Management - The management of security features and assurances through control of changes made to a system's hardware, software, firmware, documentation, test, test fixtures and test documentation throughout the development and operational life of the system. Compare configuration control.

Contingency Plan - A plan for emergency response, backup operations, and post-disaster recovery maintained by an activity as a part of its security program that will ensure the availability of critical resources and facilitate the continuity of

operations in an emergency situation. Synonymous with disaster plan and emergency plan.

Countermeasures - Any action, device, procedure, technique, or other measure that reduces the vulnerability of or threat to a system.

Cryptography - The principles, means and methods for rendering information unintelligible, and for restoring encrypted information to intelligible form.

Cryptosecurity - The security or protection resulting from the proper use of technically sound cryptosystems.

Data Encryption Standard (DES) - A cryptographic algorithm for the protection of unclassified data, published in Federal Information Processing Standard (FIPS) 46. The DES, which was approved by the National Institute of Standards and Technology, is intended for public and government use.

Data Integrity - Is the concept of being able to assure that information/data or voice transmissions can be maintained in an unimpaired condition and is not subjected to unauthorized modification whether that modification is intentional or inadvertent.

Data Security - The protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure.

Denial of Service - Any action or series of actions that prevent any part of a system from functioning in accordance with its intended purpose. This includes any action that causes unauthorized destruction, modification, or delay of service. Synonymous with interdiction.

DDD (Direct Distance Dialing) - Subscriber dialing over the nationwide intertoll telephone network.

Dial-Up - The service whereby a computer terminal can use the telephone to initiate and effect communication with a computer.

Disconnect Signal - A signal (on-hook) from the calling or called subscriber which notifies the operator or office switching equipment that the call is over and the connection should be released.

Discretionary Access Control (DAC) - A means of restricting access to objects based on the identity and need-to-know of the user, process and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps

indirectly) on to any other subject. Compare mandatory access control.

DTMF (Dual Tone Multifrequency Signalling) - A method of signalling in which a combination of two frequencies out of a possible eight are used to transmit numerical address information. The eight possible frequencies are 697, 770, 852, 941, 1209, 1336, 1477, and 1633 Hz.

End Office - The local central office at which subscriber lines and trunks are interconnected. It is designated a class 5 office in the DDD network.

End-to-End Encryption - The protection of information passed in a telecommunications system by cryptographic means, from point of origin to point of destination.

Entrapment - The deliberate planting of apparent flaws in a system for the purpose of detecting attempted penetrations.

Erasure - A process by which a signal recorded on magnetic media is removed. Erasure is accomplished in two ways: (1) by alternating current erasure, by which the information is destroyed by applying an alternating high and low magnetic field to the media; or (2) by direct current erasure, by which the media are saturated by applying a unidirectional magnetic field.

Fail Safe - Pertaining to the automatic protection of programs and/or processing systems to maintain safety when a hardware or software failure is detected in a system.

Failure Access - An unauthorized and usually inadvertent access to data resulting from a hardware or software failure in the system.

File Protection - The aggregate of all processes and procedures in a system designed to inhibit unauthorized access, contamination, or elimination of a file.

File Security - The means by which access to computer files is limited to authorized users only.

Functional Testing - The segment of security testing in which the advertised security mechanisms of the system are tested, under operational conditions, for correct operation.

In-band Signalling - The transmission of signalling information via tones at some frequency or frequencies that lie within a carrier channel normally used for voice transmission.

Identification - The process that enables recognition of an entity by a system, generally by the use of unique machine-readable user names.

Incomplete Parameter Checking - A system design flaw that results when all parameters have not been fully anticipated for accuracy and consistency, thus making the system vulnerable to penetration.

Individual Accountability - The ability to associate positively the identity of a user with the method, and degree of access to a system.

Integrity - Sound, unimpaired or perfect condition.

Internal Security Controls - Hardware, firmware, and software features within a system that restricts access to resources (hardware, software, and data) to authorized subjects only (persons, programs, or devices).

Interoffice Trunk - The telephone channel between two central offices.

Intraoffice Trunk - The trunk connection within the same central office.

Isolation - The containment of subjects and objects in a system in such a way that they are separated from one another, as well as from the protection controls of the operating system.

Least Privilege - The principle that requires that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.

Lock-And-Key Protection System - A protection system that involves matching a key or password with a specific access requirement.

Loop - The closed circuit that is formed by the subscriber's telephone and the cable pair and other conductors that make the connection to central office switching equipment.

Matrix - The place where the originating and terminating paths are tied together. The matrix holds up the talk path. An analog matrix is a 1:1 ratio. For every one conversation, there is one terminal which will be provided by the existing infotron data communications hardwired path through the switch. A digital matrix brings in 32 channels on one PCM path. Therefore, many conversations share one path.

National Computer Security Center (NCSC) - Originally named the DoD Computer Security Center, the NCSC is responsible for encouraging the

widespread availability of trusted computer system throughout the Federal Government.

Network Control - The place that sets up the matrix, identifies register, established talk path, and identifies incoming and outgoing "ports".

Object - A passive entity that contains or receives information. Access to an object potentially implies access to the information it contains. Examples of objects are: records, blocks, pages, segments, files, directories, directory trees, and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, and network nodes.

Object Reuse - The reassignment and reuse of a storage medium (e.g., page frame, disk sector, magnetic tape) that once contained one or more objects. To be securely reused and assigned to a new subject, storage media must contain no residual data (magnetic remanence) from the object(s) previously contained in the media.

Off-Hook - An off-hook condition occurs when the telephone handset is lifted from its mounting, thus causing the hookswitch to operate (close) and closing the loop to the central office. The off-hook condition indicates a busy condition to incoming calls.

Office Code - The first three digits of a seven-digit telephone number.

On-Hook - An on-hook condition exists when the telephone handset is on its mounting, thus keeping the hookswitch open. The on-hook condition opens the DC loop, indicating that calls can be accepted.

Out-of-Band Signalling - A method of signalling which uses a frequency that is within the bandwidth of the transmission facility, but outside of a carrier channel normally used for voice transmission.

Password - A protected/private character string used to authenticate an identity.

Penetration - The successful act of bypassing the security mechanisms of a system.

Penetration Signature - The characteristics or identifying marks that may be produced by a penetration.

Penetration Study - A study to determine the feasibility and methods for defeating controls of a system.

Penetration Testing - The portion of security testing in which the evaluators attempt to circumvent the security features of a system. The evaluators may be assumed to use all system design and implementation documentation, which may include listings of system source code, manuals, and circuit diagrams. The evaluators work under the same constraints applied to ordinary users.

Personnel Security - The procedures established to ensure that all personnel who have access to sensitive information have the required authority as well as appropriate clearance.

Physical Security - The application of physical barriers and control procedures as preventive measures or countermeasures against threats to resources and sensitive information.

Recovery Procedures - The actions necessary to restore a system's computational capability and data files after a system failure.

Reliability - The probability of a given system performing its mission adequately for a specified period of time under the expected operating conditions.

Remote Access - 1) Dial up access by users to a modem for access to the PBX data; 2) dial up access via DISA by subscribers to allow re-origination of calls (toll or other) from the PBX, usually accessed via a toll free number.

Restart - manual process of re-initializing (booting up) the telephone switch operating system. There are normally three types of restarts.

> **Cold Restart** - An initialization phase during which temporary storage is deallocated and cleared. All calls are dropped and the peripheral processors clear all channel assignments.
>
> **Reload Restart** - Refers to the initialization of software pointers in a program to simulate actual reload of software into the telephone switch. Office configuration and translation data is retained but all dynamic call data is cleared.
>
> **Warm Restart** - An initialization phase during which temporary storage is deallocated and cleared. Transient calls are dropped while calls in the talking state continue.

Restricted Area - Any area to which access subject to special restrictions or controls for reasons of security or safeguarding of property or material.

Restriction of Message (toll diversion) - A telephone arrangement where

outgoing calls from a private automatic branch exchange (PABX) must either be routed through an operator or are limited to specified trunk groups.

Risk Analysis - The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards. Risk analysis is a part of risk management. Synonymous with risk assessment.

Risk Management - The total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review.

Secure Configuration Management - The set of procedures appropriate for controlling changes to a system's hardware and software structure for the purpose of ensuring that changes will not lead to violations of the system's security policy.

Security Evaluation - An evaluation done to assess the degree of trust that can be placed in systems for the secure handling of sensitive information. One type, a product evaluation, is an evaluation performed on the hardware and software features and assurances of a computer product from a perspective that excludes the application environment. The other type, a system evaluation, is done for the purpose of assessing a system's security safeguards with respect to a specific operational mission and is a major step in the certification and accreditation process.

Security Features - The security-relevant functions, mechanisms, and characteristics of system hardware and software. Security features are a subset of system security safeguards.

Security Level - The combination of hierarchical classification and a set of nonhierarchial categories that represents the sensitivity of information.

Security Requirements - The types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policy.

Sensitive Information - Any information, the loss, misuse, modification of, or unauthorized access to, could affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, U.S. Code, but that has not been specifically authorized under criteria established by an Executive order or an act of Congress to be kept classified in the interest of national defense or foreign policy.

Sensitivity Label - A piece of information that represents the security level of an object.

Signalling - The process by which a caller on the transmitting end of a line informs the particular party at the receiving end that a message is to be communicated. Signalling is also supervisory information that lets callers know that called parties are ready to talk, that their line is busy, or that they have hung up. Signalling also holds the voice path while a conversation goes on.

Signalling Point (SP) - A node in a signalling network which either originates and receives signalling messages, or transfers messages from one signalling link to another, or does both.

Subset - A subscriber's telephone apparatus.

Switching Office - A location where either toll or local telephone traffic is switched or connected from one line or circuit to another. Also called switching center.

System Integrity - The quality that a system has when it performs its intended functioning in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

Tampering - An unauthorized modification that alters the prior functioning of an equipment or system in a manner that degrades the security or functionality it provides.

Technical Attack - An attack that can be perpetrated by circumventing hardware and software protection mechanisms, rather than by subverting system personnel or other users.

Technical Vulnerability - A hardware, firmware, communication, or software flaw that leaves a computer processing system open for potential exploitation, either externally or internally, thereby resulting in risk for the owner, user, or manager of the system.

Threat - Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modifications of data, and/or denial of service.

Threat Agent - A method used to exploit a vulnerability in a system, operation, or facility.

Threat analysis - The examination of all actions and events that might adversely affect a system or operation.

Threat Monitoring - The analysis, assessment, and review of audit trails and other data collected for the purpose of searching out system events that may constitute

violations or attempted violations of system security.

Token Device - A device used for generating passwords based on some information (e.g. time, date, and personal identification number) that is valid for only a brief period (e.g. 1 minute).

Trojan Horse - A computer program with an apparent or actual useful function that contains additional (hidden) functions that surreptitiously bypass the legitimate authorizations of the invoking process to the detriment of security or integrity.

User ID - A unique symbol or character string that is used by a system to identify a specific user.

User Profile - Patterns of a user's activity that can be used to detect changes in normal routines.

Verification - The process of comparing two levels of system specification for proper correspondence (e.g., security policy model with top-level specification, top-level specification with source code, or source code with object code). This process may or may not be automated.

Virus - A self-propagating malicious software program, composed of a mission component, a trigger component, and a self-propagating component.

Vulnerability - A weakness in system security procedures, system design, implementation, internal controls, etc., that could be exploited to violate system security policy.

Vulnerability Analysis - The systematic examination of systems in order to determine the adequacy of security measures, identify security deficiencies, and provide data from which to predict the effectiveness of proposed security measures.

Vulnerability Assessment - A measurement of vulnerability which includes the susceptibility of a particular system to a specific attack and the opportunities available to a threat agent to mount that attack.

Appendix A: Example Security Policy and Baseline Security Controls

1.0 Security Policy

This policy concerns the generic digital switching equipment (PBX) configuration, switch data, and maintenance and administration functions. This policy deals mainly with constraints that are enforceable through system software manipulation. Policy statements concerning physical, procedural, or administrative functions will be discussed in Baseline Security Controls.

1. The switch will route all calls only to their intended authorized destinations.

2. The switch will prevent unauthorized access to, or tampering with existing connections or conversations.

3. The switch will prevent unauthorized disconnection of calls and support positive disconnection.

4. The switch will prevent unauthorized observation or manipulation of the subscriber database within the switch memory.

5. The switch will restrict the use of its resources and features to authorized users and subscribers, and will allow only authorized users to modify switch database attributes. The switch will log all unauthorized user access attempts as well as authorized user attempts to do unauthorized functions.

6. The switch will implement valid identification and authentication procedures for physical access to switch hardware and software.

7. The switch will maintain an audit trail of all security related incidents occurring within the switch and the audit information will be protected from unauthorized access, modification, or destruction.

8. The switch will exercise the option of providing control of privileged user access to switch functions, with each user only allowed access to its specific functions necessary to perform his/her duties.

9. The switch shall define and control access to switch system objects (e.g., software modules, routing tables, configuration tables).

10. The switch will ensure that its security enforcement software shall be protected from external interference or tampering.

2.0 Baseline Security Controls

There are certain security controls that are basic to system security administration. All personnel that work directly with the PBX network should adhere to these controls to enhance the organization's security posture.

2.1 Manual Assurance of Database Integrity

Each person associated with the PBX system has certain roles for which they are responsible. These roles are defined in maintenance, administration, or security descriptions. It is imperative that these roles are clearly defined to ensure that the person tasked will not have any other roles and privileges but those necessary to fulfill the role. It is important to ensure that there is a confirmation process for the authorized disclosure or use of PBX documents. The confirmation process could be as simple as the issuance of permits and receipts and the verification of such documents. It is important that the users of the PBX be given the responsibility for the accuracy, safekeeping, and dissemination of the specific data or documents within their control. Disclosure, or unauthorized use of documents should be prevented. Such data or documents should be reviewed for potential loss and appropriately disposed of when no longer required. Such data or documents should be properly tagged or labeled with security classification (e.g., PROPRIETARY or FOR OFFICIAL USE ONLY) and such classification will carry its own procedures for use, disclosure, or destruction.

2.2 Physical Security

The main objective is to avoid destruction of assets which in turn may cause service or business interruption. In either case, there is a corresponding monetary loss. Structures housing the PBX system should be unobtrusive and show minimum indication of its purpose. A physical security perimeter should be clearly established and maintained. PBX network equipment should be secured to ensure protection from damage and unauthorized access or use. Sensitive areas within the PBX area should be made physically secure during unattended time using such methods as locked doors, automatic detection devices, and positive identification and authentification access restrictions. Personnel traffic and access to work areas should be minimized to authorized personnel only. Sensitive areas (e.g. switchroom, file storage area, and cross-connect terminal) should be placed or positioned in low traffic areas if traffic can not be controlled.

2.3 Operations Security

The objective is to prevent compromise of PBX data. Applications, patches, supplements, and test programs are usually needed to test and upgrade the PBX system. In this regard, the PBX administrator will sometimes need to provide accurate real-time data to the firmware software developers or programmers. Sensitive data should be properly handled in a manner befitting its classification. Proper care should be exercised to

minimize exposure of all PBX data not needed for the specific problems. Operations security also involves protection against unauthorized software or hardware modifications. It also involves prevention of trouble calls being overlooked, especially the ones that deals directly to PBX integrity (e.g. network integrity, memory mismatches, and carrier loss). All activity initiated within the PBX system should be logged and a record kept of this log. This log will encompass not only normal daily operational routines but also maintenance and trouble shooting procedures. If a problem was found and subsequently fixed, the steps involved in the whole procedure should be put in the log. Another objective is to detect unauthorized system use. Most PBX systems have within its security parameters the method to record, in memory, items such as system activity logs, journal files, exception reports, software errors, hardware errors, and operations and measurements parameters. These parameters or files should be constantly checked and updated, both manually and automatically. Back-ups of system configuration and database should be kept and maintained at least daily. Such back-up files should be kept in a secure area allowing access only by authorized personnel.

2.4 Management Initiated Controls

The objectives are to prevent loss of security support; prevent disclosure, taking, or unauthorized use of documents; and prevent inadequate PBX system controls. Personnel accountable for the security of the PBX should require that these areas are explicitly defined. PBX administration requires the use and filing of reports and other documents which includes security reviews, audits, PBX traffic reports, subscriber trouble reporting logs, and maintenance logs. These reports are sensitive and should be protected. Management should also be aware that there are other PBX owners/users and that they may have devised other ways of protecting their investments.

2.5 PBX System Control

The objectives are to avoid inadequacy of controls, to detect PBX systems and operations failures, and to prevent loss, modification, disclosure, or destruction of switch data assets. Third party vendor supplied PBX support programs (e.g. call detail recording systems) should be used without modification. Many of these programs have been developed with the controls and integrity built into them. Any modifications may possibly compromise its built in capabilities. Whenever changes are to be made in the PBX switch database or operating system, a review of the change should be made to make sure the new changes are necessary and will not compromise controls and integrity of the switch, have an unanticipated impact on some other part of the system, and/or interfere excessively with the existing system. Exception reporting on a periodic basis should be activated to report any deviations from the normal activity that may indicate errors or unauthorized acts. Exception reporting should occur when a specific control is violated, or may constitute a warning of possible undesirable events. Exception reporting should be recorded in a recoverable form within the system and when required, displayed to the PBX security administrator. Validation of all inputs to the PBX system should be performed, if it is not

already automatic within the PBX, to assist in the assurance of correct and proper data entry. Validation should include checking for out-of-range values, invalid characters, and excess in upper/lower limits of possible entry.

2.6 PBX System Terminal Access Control

The objective is to prevent and avoid PBX system access exposure and control access to the PBX system database. Limiting the access to the PBX system and its database is an important means of security. It may be possible to control dial-up access to the PBX for maintenance and administration purposes. A PBX port interfaced to the Public Switched Telephone Network is exposed to access from telephones anywhere in the world. There may be a trade-off between PBX security and maintenance and administration accessibility. One alternative is to restrict access to the dial-up line to certain times of the day. Dial-up modem lines should be password or access code protected. Once access is given, whether via dial-up modem lines or on-site operations, administration, and maintenance terminals, care should be taken so that only authorized personnel are allowed access to data assigned to them. Users and others who have access to the PBX database should only be allowed to view, change, or manipulate the data that pertain to their specific job functions. Different types of database read and write privileges should be given to users with different job functions. Passwords to the PBX should be kept secret. It should be set up so that each user has a distinct and separate password of their own. This is to keep positive track of their activities. Access to the use of all terminals should be restricted to authorized users. This can be done by physically securing areas in which the terminals are located.

Password Management - Password control is essential to good security. Passwords should be controlled so that they expire after a period of time (e.g. 30 days). This type of password is considered reusable and is vulnerable if the password is seen (watched being entered) or monitored. To prevent this type of vulnerability, a device to generate a password based on some information (e.g. time, date, and personal identification number) that is valid for only a brief period (e.g. 1 minute). This type of device mitigates the reusable password problems but can isolate the user if the 'token device' is lost, stolen, broken, or the batteries expire (the batteries can not be changed by the user).

Appendix B: Security Assessment Checklist

1.0 Guideline

This guideline will assist PBX network administrators in making a self-assessment of the PBX network security posture. This guideline is meant to be comprehensive but should not be construed as exhaustive. The objective is to assess and develop a security program, identify security areas that need management attention, and conduct a detailed evaluation of the current security policies.

2.0 Organizational Policy

1. Is there a published security policy for the protection of people, property, and information assets?

2. Does it contain explicit instructions?

3. Is it reviewed periodically to ensure its validity against current conditions?

4. Are assessments done to evaluate compliance with the policy?

5. Is there a person whose major function is to implement the policy?

6. Is this person trained in information and telecommunications security?

7. Are all personnel regularly advised on telecommunications security?

3.0 Physical Security

1. Is the building housing the telephone equipment protected by fire-suppression systems?

2. Are areas containing the PBX equipment equipped with appropriate automatic fire-suppression system?

3. Are personnel aware of proper fire emergency procedures?

4. Are there appropriate alarms?

5. Are telephone equipment rooms located for ease of access only to authorized personnel?

6. Is access to sensitive areas regulated?

7. Has the risk of intrusion been reviewed and adequately protected?

8. Are backups stored in a location remote from the system?

4.0 Controls and Procedures

1. At the individual level, are job functions separated from each other and from use of each others system or equipment?

2. Are duties within each of these job functions separated to a degree appropriate for the proper and efficient operation of the telephone system?

3. Are job functions assigned so that it is possible to account for each individual's actions?

4. Are all personnel aware of the inherent security threats and vulnerabilities and how to compensate for them?

5. Is responsibility for the security and protection of each equipment and resource explicitly assigned per individual?

6. Are there procedures to ensure the timely detection of fraud and abuse?

7. Is there a policy about who may access and update the telephone database?

8. Is each individual user uniquely identified to the telephone system?

9. Are dial-up ports protected from unauthorized access?

10. Are there provisions for the protection of data or voice transmissions?

11. Do controls exist to ensure programs or software do only what is intended?

12. Are all personnel regularly trained in their security roles?

13. Are all resources receiving at least minimum protection appropriate to their sensitivity?

17. Are telephone system software, database, and system memory backed up at regular intervals?